AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA

ALUMNO: SERGIO LUCENA PRATS
TUTOR: MIGUEL ÁNGEL RAMOS

Marzo de 2006

A Miguel Ángel Ramos,
por su ayuda.

A mis padres y mi familia,
por permitirme realizar esta carrera.

A Rosa,
por estar ahí.

Gracias.

ÍNDICE DE CONTENIDOS

0 - INTRODUCCIÓN

La información que tiene una entidad almacenada, que posiblemente sea el fruto de años de trabajo, es con toda probabilidad su activo más valioso, ya que si se perdieran toda la información referente a los clientes, a los proveedores o a la actividad que la entidad realiza, es posible que no se pudiera continuar.

Tradicionalmente esta información se almacenaba en grandes ficheros, pero con la implantación de los sistemas informáticos, hoy en día se hace en ordenadores. Esto ha facilitado que el nivel de información que se maneja sea mucho mayor, ya que en un simple PC se pude almacenar la misma información que en varias toneladas de papel. Con este aumento de información se ha aumentado enormemente la dependencia de las entidades hacia esta, hasta llegar al punto actual, donde es imposible prosperar en cualquier campo sin un buen sistema de información.

Puesto que el valor de la información ha aumentado, también lo han hecho sus amenazas. Hace 3 o 4 décadas a ningún empresario se le podía ocurrir que le robaran un archivo con sus clientes, sin embargo hoy día, esta información es un objetivo de ladrones como cualquier otro.

Otro factor importante que ha hecho que sean más las amenazas hacia la información es el propio desconocimiento de los sistemas informáticos empleados en las entidades. A nadie se le escapa como manejar y proteger y fichero de datos en papel, pero un gran sistema informático depende de una cantidad de factores enorme para su buen funcionamiento.

Sin embargo, aún hoy en día, muchos empresarios y altos cargos de grandes entidades no dan a la información la importancia que tiene, por lo que no conocen las posibles amenazas que pueden ponerla en peligro, ni los sistemas que existen para asegurarla.

El objetivo de éste trabajo es primeramente analizar qué elementos son los que se deben proteger para asegurar la información, así como las posibles amenazas y sistemas para contrarrestarlas. Existen muchos ámbitos y aspectos de la información y los sistemas informáticos que se pueden analizar, no obstante, en este trabajo, vamos a ver los concernientes a la seguridad física.

Se ha optado por este tema por ser muchas veces un aspecto olvidado. Aunque se empleen millones de euros en idear un sistema de cifrado que impida a un atacante robar la información de una entidad conectándose a través de la red, si un intruso puede acceder a la entidad y llevarse un servidor de datos bajo el brazo, el esfuerzo realizado habrá sido inútil.

El ejemplo que se ha puesto es un poco exagerado, pero aunque existen ciertos factores de la seguridad física, como el control de accesos o intrusiones o los sistemas antiincendios que se tienen más presentes, existen otros muchos que no están aún olvidados, como puede ser la redundancia eléctrica. Sin un sistema de éste tipo puede que una entidad que realice un gran esfuerzo en seguridad pierda toda o parte de su información ante simple corte en el suministro eléctrico. Por ello, este trabajo pretende hacer un repaso general a todas las amenazas físicas que pueden poner en peligro los sistemas de información y los medios existentes para hacerlas frente.

Precisamente por lo complejo de los sistemas informáticos y de todos los factores que se deben contemplar, se ha creado la auditoría informática, ya que es necesario que expertos en la informática y en la seguridad realicen una revisión independiente y objetiva del estado de estos sistemas. Vamos a ver en éste trabajo, por tanto, el cómo y el porqué de la auditoría informática, realizando un estudio más detallado y viendo las características concretas de la auditoría informática de la seguridad física. Se realizará un cuestionario, una aplicación informática y un caso práctico.

1 - SEGURIDAD

1.1 - ¿Qué entendemos por seguridad?

Podemos entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese sistema esta libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible.

Es muy difícil de conseguir seguridad total, por lo que podemos hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él). Se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

Como ejemplo cabe mencionar dos definiciones de seguridad:

> *"Calidad de estar libre y cubierto de **todo** riesgo"*
> Diccionario de la Real Academia Española de Lengua.

La seguridad absoluta es inalcanzable. Llega un momento en el que los gastos en seguridad dejan de ser rentables. La seguridad absoluta tendría un costo infinito.

Por el contrario

> *"Calidad **relativa** resultado del **equilibrio** entre el riesgo (constituido por amenazas, vulnerabilidades e impacto) y las medidas adoptadas para paliarlo"*
> Arturo Ribagorda. Seguridad en unix. Sistemas abiertos en Internet, Paraninfo S.A.

Ésta es una definición mucho más amplia, dice que si el riesgo es grande las medidas que se tomarán para paliarlo serán extremas, por el contrario si el riesgo es pequeño, las medidas serán pequeñas. También se tendrá que tener presente la repercusión que tendría el que cierto elemento quede desprotegido. Las medidas de seguridad han de ser proporcionales a los medios que queremos proteger.

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos:

a) Confidencialidad: La información sólo debe ser conocida por los usuarios, entidades o procesos autorizados en el tiempo y forma previstos. Podemos indicar que cuando la información hace referencia a datos de carácter personal, se podría denominar **privacidad**, aunque éste término nos indica que el individuo tiene derecho a controlar la recogida y almacenamiento de los datos.

b) Integridad: La información solo debe ser alterada o modificada por los usuarios autorizados y registrada para posteriores controles o auditorias. La información debe ser exacta y completa.

c) Disponibilidad: Los usuarios deben poder acceder a la información en el tiempo y la forma autorizada. Esto requiere que la información se mantenga correctamente almacenada.

1.2 - ¿Qué queremos proteger?

Ahora vamos a ver de forma general cuales son los principales elementos informáticos que se van a proteger. En cualquier sistema informático existen generalmente tres elementos principales a proteger, que son el **software**, el **hardware** y los **datos**, y últimamente se está incorporando un cuarto elemento, los **fungibles**.

a) Hardware

Por hardware entendemos el conjunto formado por todos los elementos físicos de un sistema informático, como los CPUs y sus componentes, terminales, cableado, medios de almacenamiento secundario como cintas, CD-ROMs o disquetes. El valor añadido que tiene el hardware es que si alguien sustrae un CPU, se llevará consigo además todos los datos que contenga su disco duro.

b) Software

El software es el conjunto de programas lógicos que hacen funcional al hardware, tanto sistemas operativos como aplicaciones.

c) Datos

Por datos entendemos el conjunto de información dispuesta de manera adecuada para su tratamiento que manejan el software y el hardware, como por ejemplo entradas de una base de datos, paquetes que circulan por un cable de red o proyectos o informes desarrollados por la entidad.

Por extensión, los datos de una entidad pueden estar informatizados o no, es decir, entenderemos también por datos las fichas de los empleados escritas en papel que una entidad conserva en un fichero. Sin embargo en este trabajo nos centraremos en los sistemas informáticos.

Como veremos más adelante, los datos son el elemento principal a proteger.

d) Fungibles

El cuarto elemento, del que se habla generalmente en las auditorías de seguridad, los fungibles, son elementos que se gastan o desgastan con el uso continuo, como papel de impresora y su tóner o tinta o cabezales de impresión. También se pueden denominar fungibles a los CDs, CD-ROMs, cintas y disquetes.

Habitualmente **los datos** constituyen el principal elemento de los cuatro a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar y es el que es el que mayor repercusión puede tener en una entidad: con toda seguridad una máquina está ubicada en un lugar de acceso físico restringido, y cuanto mayor valor económico tenga, más controlada estará. En caso de pérdida de una aplicación o un programa de sistema, podremos restaurar este software sin problemas desde su medio original, por ejemplo, el CD-ROM con el que se utilizó para su instalación o solicitándolo al proveedor.

Sin embargo, en caso de pérdida de una base de datos o de un proyecto de un usuario, no tenemos un medio "original" desde el que restaurar; hemos de pasar obligatoriamente por un sistema de copias de seguridad, y a menos que la política de copias sea muy estricta, es difícil devolver los datos al estado en que se encontraban antes de la pérdida. Además en muchas ocasiones los datos son el fruto de muchos años de trabajo de una entidad, por lo que su pérdida total podría significar, incluso, la quiebra.

De los datos podemos decir también que, además del trastorno que supondría para la entidad la pérdida, robo o deterioro de proyectos o bases de datos, existen los llamados **datos especialmente protegidos**, que son datos de carácter personal y su clasificación depende de la legislación aplicable en cada lugar y circunstancia. En el caso de la legislación española, se ajusta a los dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (B.O.E. Nº 298, de 14 de diciembre de 1999) y en el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (B.O.E. Nº 151, de 25 de junio de 1999).

1.3 - ¿De qué nos queremos proteger?

De nuevo, vamos a ver de forma general las posibles amenazas a la seguridad. Más adelante vamos a ver los relativos a la Seguridad Física de manera mucho más concreta.

Como en la mayoría de las publicaciones que se hacen sobre seguridad informática, vamos a intentar clasificar los diferentes elementos que pueden atacar nuestro sistema. Con frecuencia, especialmente en las obras menos técnicas y más orientadas a otros aspectos de la seguridad, se suele identificar a los atacantes únicamente como personas; esto tiene sentido si hablamos por ejemplo de responsabilidades por un delito informático.

Pero en este trabajo es preferible hablar de "elementos" y no de personas: aunque a veces lo olvidemos, nuestro sistema puede verse perjudicado por múltiples entidades aparte de humanos, como por ejemplo programas o fallos de hardware, y como veremos más en profundidad en el apartado de Seguridad Física, catástrofes naturales, incendios o inundaciones; si una empresa pierde la base de datos de todos sus clientes, poco le importará que haya sido un intruso, un virus, un simple error del hardware o una inundación (salvo quizá por temas de seguros y lo que esté cubierto, etc.).

Para hacernos una pequeña idea, se muestran a continuación varias agrupaciones de los elementos que pueden atacar nuestra entidad. No pretende ser exhaustiva, simplemente

trata de proporcionar una idea acerca de qué o quién amenaza un sistema. A lo largo de este proyecto se ahondará en aspectos de algunos de los elementos presentados aquí.

Clasificaciones dependiendo de:

a) Su origen:

i) Naturales. Se producen de manera espontánea y son causadas por fenómenos naturales.

i.i) Terremotos. Aunque casi inexistentes en España, hasta los pequeños temblores pueden provocar grandes pérdidas.
i.ii) Tormentas eléctricas. Pueden provocar daños eléctricos, así como incendios y otros daños.
i.iii) Temperatura. Las temperaturas extremas, sobre todo el calor, pueden provocar daños y malfuncionamiento en los equipos
i.iv) Humedad. Al igual que la temperatura, puede dañar seriamente los equipos eléctricos.
i.v) Lluvias. Pueden ser la causa de inundaciones.
i.vi) Otros Factores. Menos importantes, pueden ser el viento, el granizo, etc.

ii) Accidentales. Son los que se producen de manera espontánea pero no son cusa de la naturaleza.

ii.i) Errores humanos (accidentes). Tiene una importancia alta y son muy comunes. Pueden afectar a casi todos los factores de seguridad de la entidad.
ii.ii) Fallos en equipos (hardware). Son poco habituales.
ii.iii) Malfuncionamiento de programas (software). Son bastante habituales e importantes.
ii.iv) Radiaciones electromagnéticas. Son poco habituales, pero dada la creciente red de tecnologías Wi-Fi y móviles, va muy en aumento.

iii) Deliberadas o Intencionadas. Son las que se producen a propósito. Pueden tener múltiples fines.

iii.i) Fraudes. Son muy frecuentes.
iii.ii) Sabotajes. Pueden ser materiales (como la rotura de los canales de comunicaciones, etc.) o inmateriales (por medio de virus, etc.).

iii.iii) Hurtos. Igualmente pueden ser materiales (los que todos conocemos, equipos, dinero, etc.) o inmateriales (robo de software, datos, etc.).

b) Su actuación:

i) Pasivas. No alteran el estado de la información por lo que son las más difíciles de descubrir. Amenazan a la confidencialidad.

i.i) Interceptación. Leen nuestra información, por ejemplo, pinchando una línea de datos.
i.ii) Copia. Hacen una copia de los datos desde el sitio físico en el que se encuentran.

ii) Activas. Estas alteran el estado de la información.

ii.i) Interrupción. Amenaza la disponibilidad. Por ejemplo, cortando el cable de datos, la red eléctrica, etc.
ii.ii) Modificación (de los datos). Amenaza la integridad. Por ejemplo, entrando en el sistema (remotamente o desde el lugar físico).
ii.iii) Fabricación. Generar datos o software e integrarlos en el sistema. Afecta a la integridad.
ii.iv) Destrucción. Borran o destruyen documentos, equipos o software de la entidad.

c) Su procedencia:

i) Errores internos. Fuente de mayores pérdidas en conjunto. Provocada por la aparición de errores en el software, hardware, sistemas de ventilación, errores humanos, etc.

ii) Empleados infieles. Por múltiples motivos: empleados descontentos, intereses económicos, etc.

iii) Desastres. Son los menos habituales, pero si no se está preparado, son los más destructivos. Por ejemplo una inundación o un incendio.

iv) Acciones de terceros. Vienen del exterior de la entidad. Tienen múltiples orígenes y objetivos y pueden ser intencionados o no.

Esquema 1.1

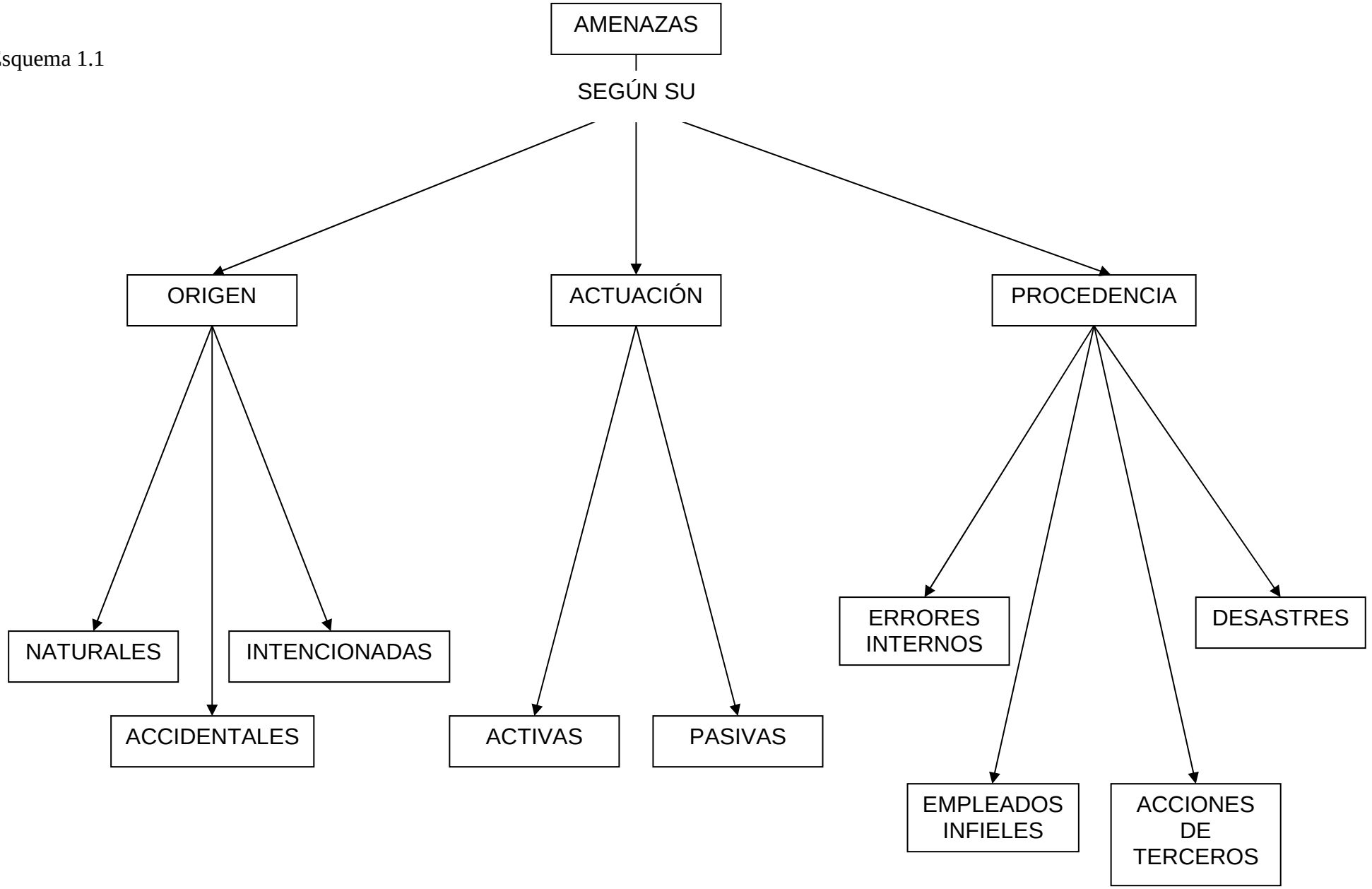
Una vez vistas estas clasificaciones, podemos establecer que un elemento que amenaza la seguridad de una entidad pertenece a un tipo de cada una de las agrupaciones. Así, vamos a ver un **ejemplo:**

Una excavadora que haciendo una carretera, corta por descuido del conductor un canal de comunicaciones de la entidad o de la compañía que nos provee las comunicaciones.

Según su origen, accidental y pertenecerá al grupo de errores humanos.
Por su actuación, dentro de las activas, interrupción.
Según su procedencia, será una acción de terceros, externa a la entidad.

Dependiendo del caso en concreto, cada amenaza pertenecerá a un tipo de los anteriormente mencionados. Puede que una misma amenaza, por ejemplo, un incendio, tenga distintos objetivos u orígenes, que se genera en la entidad o fuera de ésta y por accidente o intencionadamente. Dependiendo de todos estos factores, la entidad actuará de una manera o de otra.

Esquema 1.1


AMENAZAS
SEGÚN SU
ORIGEN
ACTUACIÓN
PROCEDENCIA
NATURALES
INTENCIONADAS
ACCIDENTALES
ACTIVAS
PASIVAS
ERRORES INTERNOS
DESASTRES
EMPLEADOS INFIELES
ACCIONES DE TERCEROS

1.4 - Elementos que comprometen la seguridad

Como ya hemos mencionado, más adelante vamos a profundizar en la Seguridad Física, y por tanto, también sus posibles atacantes, pero para hacernos una idea de los posibles elementos que comprometen la seguridad de una entidad, vamos a dar un repaso de estos. Creo que es interesante conocer estas amenazas como tal un poco más en profundidad.

a) Personas:

Hay que tener muy presente que la mayoría de ataques a nuestra entidad van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas. A nivel lógico, podemos hablar de piratas que, con distintos fines, intentan conseguir el control o acceso a los sistemas aprovechando alguno de los riesgos lógicos (de los que hablaremos a continuación), especialmente agujeros del software. Pero con demasiada frecuencia se suele olvidar que los piratas "clásicos" no son los únicos que amenazan nuestros equipos. Es especialmente preocupante que mientras que hoy en día cualquier administrador mínimamente preocupado por la seguridad va a conseguir un sistema relativamente fiable de una forma lógica (permaneciendo atento a vulnerabilidades de su software, restringiendo servicios, utilizando cifrado de datos, etc.), pocos administradores tienen en cuenta factores físicos**,** como el acceso a la sala donde existen elementos vulnerables o un buen sistema de recuperación de datos, ya que podemos ser víctimas de sabotajes.

Aquí se describen brevemente los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas; generalmente se dividen en dos grandes grupos: los atacantes pasivos, aquellos que fisgonean por el sistema pero no lo modifican (o destruyen), y los activos, aquellos que dañan el objetivo atacado, o lo modifican en su favor. Generalmente los curiosos y los crackers realizan ataques pasivos (que se pueden convertir en activos), mientras que los terroristas y ex-empleados realizan ataques activos puros; los intrusos remunerados suelen ser atacantes pasivos si nuestra red o equipo no es su objetivo, y activos en caso contrario. El personal realiza ambos tipos indistintamente, dependiendo de la situación concreta.

i) Personal

Las amenazas a la seguridad de un sistema provenientes del personal de la propia entidad rara vez son tomadas en cuenta; se presupone un entorno de confianza donde a veces no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la entidad, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento, etc.) puede comprometer la seguridad de los equipos, los datos y la entidad en general.

Lo más normal es que más que de ataques se trate de accidentes causados por un error o por desconocimiento de las normas básicas de seguridad: un empleado de mantenimiento que corta el suministro eléctrico para hacer una reparación o un cigarrillo olvidado pueden ser tanto o más peligrosos como el más experto de los administradores que se equivoca al teclear una orden y borra todos los sistemas de ficheros. En los dos primeros casos, los "atacantes" ni siquiera han de tener acceso lógico (ni físico) a los equipos, ni conocer nada sobre seguridad.

Sin embargo, los ataques intencionados son extremadamente dañinos y peligrosos, recordemos que nadie mejor que el propio personal de la entidad conoce mejor los sistemas y sus debilidades. Estos pueden deberse a múltiples cusas, pero el soborno de terceros a personal de la entidad para conseguir datos o accesos es lo más normal. Los ataques llevados acabo por el personal de la entidad tiene además la característica de que pueden no ser descubiertos jamás.

ii) Ex-empleados

Otro gran grupo de personas potencialmente interesadas en atacar nuestra entidad son los antiguos empleados o trabajadores de la misma, especialmente los que no abandonaron el entorno por voluntad propia (y en el caso de redes de empresas, los que pasaron a la competencia). Generalmente, se trata de personas descontentas con la entidad, conocen y han tenido acceso previo al sistema y pueden intentar acceder a él para dañarlo como venganza por algún hecho que no consideran justo, para obtener información y venderla a terceros o incluso para modificar datos de cuentas y nominas de la entidad y así seguir cobrando como si aún trabajaran para ésta. Además pueden obtener información delicada para la entidad o para el personal, y de esta manera chantajear a sus ex-jefes o ex-compañeros.

Podemos incluir en este grupo a personas externas a la entidad, que han trabajado para ésta o con ésta y tienen conocimiento del sistema, incluso de las contraseñas de acceso. Por eso es muy importante que la entidad permita el acceso al sistema sólo durante el periodo de tiempo necesario y sepa en todo momento quién y cuándo accede.

iii) Curiosos

Junto con los crackers, los curiosos son los atacantes más habituales de sistemas informáticos. Suelen ser personas ajenas al sistema pero con curiosidad por la seguridad del mismo. No suelen tener malas intenciones.

Teniendo en cuenta que tanto futuros profesionales de la informática y las telecomunicaciones como profesionales ya consagrados en éstas áreas, son personas que a priori tiene mucho interés por las nuevas tecnologías; y recordemos que las personas suelen ser curiosas por naturaleza. Esta combinación produce una avalancha de estudiantes o personal intentando conseguir mayor privilegio del que tienen o intentando acceder a sistemas a los que oficialmente no tienen acceso. Y en la mayoría de ocasiones esto se hace simplemente para leer el correo de un amigo, enterarse de cuánto cobra un compañero, copiar un trabajo o comprobar que es posible romper la seguridad de un sistema concreto. Aunque en la mayoría de situaciones se trata de ataques no destructivos (a excepción del borrado de huellas para evitar la detección), parece claro que no benefician en absoluto al entorno de fiabilidad que podamos generar en un determinado sistema.

iv) *Crackers*

Su objetivo es romper el sistema de seguridad. Están especializados en sistemas de protección de software de seguridad media, aunque sus técnicas se utilizan también para romper sistemas de protección de acceso a aplicaciones. Estos entornos de seguridad media (redes de I+D, universidades, etc.) son un objetivo típico de los intrusos, ya sea para fisgonear, para utilizarlas como enlace hacia otras redes o simplemente por diversión. Por un lado, son redes generalmente abiertas, y la seguridad no es un factor

tenido muy en cuenta en ellas; por otro, el gran número y variedad de sistemas conectados a estas redes provoca, casi por simple probabilidad, que al menos algunos de sus equipos (cuando no la mayoría) sean vulnerables a problemas conocidos de antemano. De esta forma un atacante sólo ha de utilizar un escáner de seguridad contra el dominio completo y luego atacar mediante un simple *exploit*(1) los equipos que presentan vulnerabilidades.

Esto convierte a las redes de I+D, a las de empresas, o a las de *ISPs*(2) en un objetivo fácil y apetecible para piratas con cualquier nivel de conocimientos, desde los más novatos (y a veces más peligrosos) hasta los expertos, que pueden utilizar toda la red para probar nuevos ataques o como nodo intermedio en un ataque a otros organismos, con el consiguiente deterioro de imagen (y a veces de presupuesto) que supone para una universidad ser, sin desearlo, un apoyo a los piratas que atacan sistemas teóricamente más protegidos, como los militares.

(1) (Viene de *to exploit* - aprovechar) Programa o técnica que aprovecha un error de programación para obtener diversos privilegios.
(2) *Internet Service Provider*. Hace referencia al sistema informático remoto al cual se conecta un ordenador personal y a través del cual se accede a Internet.

v) Terroristas
Por "terroristas" no debemos entender simplemente a los que se dedican a poner bombas o quemar autobuses; bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él. Por ejemplo, alguien puede intentar borrar las bases de datos de un partido político enemigo o destruir los sistemas de ficheros de un servidor que alberga páginas WEB de algún grupo religioso. En el caso de redes de I+D, típicos ataques son la destrucción de sistemas de prácticas o la modificación de páginas WEB de algún departamento o de ciertos profesores, generalmente por parte de alumnos descontentos. Su principal objetivo es por tanto, la destrucción.

vi) Intrusos remunerados
Este es el grupo de atacantes de un sistema más peligroso, aunque por fortuna el menos habitual en redes normales; suele afectar más a las grandes - muy grandes - entidades o a organismos de defensa. Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que son pagados por una tercera parte generalmente para robar secretos (el nuevo diseño de un procesador, una base de datos de clientes, información confidencial sobre las posiciones de satélites espía, etc.) o simplemente para dañar la imagen de la entidad afectada. Esta tercera parte suele ser una empresa de la competencia o un organismo de inteligencia, es decir, una organización que puede permitirse un gran gasto en el ataque; de ahí su peligrosidad: se suele pagar bien a los mejores piratas y, por si esto fuera poco, los atacantes van a tener todos los medios necesarios a su alcance.

b) Amenazas lógicas

Bajo la etiqueta de "amenazas lógicas" encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello

(software malicioso, también conocido como *malware*[3]) o simplemente por error (*bugs*[4] o agujeros).

[3] (Viene de *malicius software*) Son programas o archivos dañinos para el ordenador, están diseñados para insertar virus, gusanos, troyanos o *spyware* para conseguir algún objetivo, como podría ser el de recoger información sobre el usuario o sobre el ordenador en sí.
[4] Error de software, resultado de un fallo de programación en el proceso de creación del software.

i) Software incorrecto
Las amenazas más habituales a un sistema informático provienen de errores cometidos de forma involuntaria por los programadores de sistemas operativos o de aplicaciones. Una situación no contemplada a la hora de diseñar el sistema de red o un error accediendo a memoria en un fichero pueden comprometer local o remotamente al sistema.

A estos errores de programación se les denomina *bugs* (agujeros), y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, *exploits*. Como hemos dicho, representan la amenaza más común contra los sistemas, ya que cualquiera puede conseguir un *exploit* y utilizarlo contra nuestra máquina sin ni siquiera saber cómo funciona y sin unos conocimientos mínimos. Incluso, hay *exploits* que dañan seriamente la integridad de un sistema (negaciones de servicio o accesos privilegiados remotos) y están preparados para ser utilizados desde cualquier sistema operativo y sin ningún conocimiento de informática, con lo que cualquier pirata novato o *Script Kiddie*[5] puede utilizarlos contra un servidor y conseguir un control total de una máquina de varios millones de pesetas desde su PC, sin saber nada del sistema atacado.

[5] Persona que presume de ser un *hacker* o *cracker* cuando en realidad no posee un grado de conocimientos suficientes. Normalmente usa *cracks*, *exploits* y programas similares construidos por personas con grandes conocimientos pero cuyo uso está al alcance de cualquiera.

ii) Herramientas de seguridad
Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. Herramientas como NESSUS, SAINT o SATAN pasan de ser útiles a ser peligrosas cuando las utilizan *crackers* que buscan información sobre las vulnerabilidades de un *host*[6] o de una red completa.

[6] Cualquier máquina conectada a una red de ordenadores

La conveniencia de diseñar y distribuir libremente herramientas que puedan facilitar un ataque es un tema peliagudo; incluso expertos reconocidos como Alec Muffet (autor del adivinador de contraseñas *Crack*) han recibido enormes críticas por diseñar determinadas herramientas de seguridad. Tras numerosos debates sobre el tema, ha quedado bastante claro que no se puede basar la seguridad de un sistema en el supuesto desconocimiento de sus problemas por parte de los atacantes: esta política, denominada *Security Through Obscurity*, se ha demostrado inservible en múltiples ocasiones. Si

como administradores no utilizamos herramientas de seguridad que muestren las debilidades de nuestros sistemas (para corregirlas), tenemos que estar seguro que un atacante no va a dudar en utilizar tales herramientas (para explotar las debilidades encontradas); por tanto, hemos de agradecer a los diseñadores de tales programas el esfuerzo que han realizado (y nos han ahorrado) en pro de sistemas más seguros.

iii) Puertas traseras

Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar "atajos" en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denomina puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos: por ejemplo, los diseñadores de un software de gestión de bases de datos en el que para acceder a una tabla se necesiten cuatro claves diferentes de diez caracteres cada una pueden insertar una rutina para conseguir ese acceso mediante una única clave "especial", con el objetivo de perder menos tiempo al depurar el sistema. Algunos programadores pueden dejar estos atajos en las versiones definitivas de su software para facilitar un mantenimiento posterior, para garantizar su propio acceso, o simplemente por descuido; la cuestión es que si un atacante descubre una de estas puertas traseras (no nos importa el método que utilice para hacerlo) va a tener un acceso global a datos que no debería poder leer, lo que obviamente supone un grave peligro para la integridad de nuestro sistema.

iv) Bombas lógicas

Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial. Los activadores más comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos ficheros, la ejecución bajo un determinado *login* o la llegada de una fecha concreta; cuando la bomba se activa va a poder realizar cualquier tarea que pueda realizar la persona que ejecuta el programa: si las activa el administrador los efectos obviamente pueden ser fatales.

v) Canales cubiertos

Los canales cubiertos (o canales ocultos, según otras traducciones) son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; dicho de otra forma, un proceso transmite información a otros (locales o remotos) que no están autorizados a leer dicha información. Los canales cubiertos no son una amenaza demasiado habitual en redes de I+D, ya que suele ser mucho más fácil para un atacante aprovechar cualquier otro mecanismo de ataque lógico; sin embargo, es posible su existencia, y en este caso su detección suele ser difícil: algo tan simple como el puerto *finger*[(7)] abierto en una máquina puede ser utilizado a modo de canal cubierto por un pirata con algo de experiencia.

[(7)] Puerto que permite saber qué usuarios están conectados a la máquina. Se puede acceder a él por telnet.

vi) Virus

Un virus es una secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

En mayor o menor medida, todo el mundo conoce, incluso a padecido los efectos de los virus. Estos efectos son muy variados: formatear el disco duro, dañar el sector de arranque del PC, hacer que se reinicie, dañar algunos programas en concreto, mal funciones de video, etc. La mayoría de los efectos son perceptibles por el usuario, si bien existen virus que pueden actuar de manera más "silenciosa" haciendo que se relentice el sistema o se desconfigure. Esto podría dar más problemas, ya que si el usuario no sabe que está infectado no pondrá medios para subsanar este problema.

vii) Gusanos

Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando *bugs* de los sistemas a los que conecta para dañarlos. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande: el mayor incidente de seguridad en Internet fué precisamente el *Internet Worm*, un gusano que en 1988 causó perdidas millonarias al infectar y detener más de 6.000 máquinas conectadas a la red.

Hemos de pensar que un gusano puede automatizar y ejecutar en unos segundos todos los pasos que seguiría un atacante humano para acceder a nuestro sistema: mientras que una persona, por muchos conocimientos y medios que posea, tardaría como mínimo horas en controlar nuestra red completa (un tiempo más que razonable para detectarlo), un gusano puede hacer eso mismo en pocos minutos: de ahí su enorme peligro y sus devastadores efectos.

iix) Caballos de Troya

Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario; como el Caballo de Troya de la mitología griega, al que deben su nombre, ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.

De esta manera, cuando un intruso penetra en el sistema, instala troyanos para no ser descubierto o garantizarse el poder volver a entrar. Estos troyanos sustituyen a los programas habituales del sistema de modo que el usuario no se percate de que el atacante se encuentra conectado a su sistema.

ix) Programas conejo o bacterias

Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco, etc.), produciendo una negación de servicio. Por sí mismos no hacen ningún daño, sino que lo que realmente perjudica es el gran número de copias suyas en el sistema, que en algunas situaciones pueden llegar a provocar la parada total de la máquina.

Hemos de pensar que hay ciertos programas que pueden actuar como conejos sin proponérselo; ejemplos típicos se suelen encontrar en los sistemas destinados a prácticas en las que se enseña a programar al alumnado: es muy común que un bucle que por error se convierte en infinito contenga entre sus instrucciones algunas de reserva de memoria, lo que implica que si el sistema no presenta una correcta política de cuotas

para procesos de usuario pueda venirse abajo o degradar enormemente sus prestaciones. El hecho de que el autor suela ser fácilmente localizable no debe ser ninguna excusa para descuidar esta política: no podemos culpar a un usuario por un simple error, y además el daño ya se ha producido.

x) Técnicas salami

Por técnica salami se conoce al robo automatizado de pequeñas cantidades de bienes (generalmente dinero) de una gran cantidad origen. El hecho de que la cantidad inicial sea grande y la robada pequeña hace extremadamente difícil su detección: si de una cuenta con varios millones de euros se roban unos céntimos, nadie va a darse cuenta de ello; si esto se automatiza para, por ejemplo, descontar unos céntimos de cada nómina pagada en la universidad o de cada beca concedida, tras un mes de actividad seguramente se habrá robado una enorme cantidad de dinero sin que nadie se haya percatado de este hecho, ya que de cada origen se ha tomado una cantidad ínfima.

Las técnicas salami no se suelen utilizar para atacar sistemas normales, sino que su uso más habitual es en sistemas bancarios; sin embargo, como en una red con requerimientos de seguridad medios es posible que haya ordenadores dedicados a contabilidad, facturación de un departamento o gestión de nóminas del personal, comentamos esta potencial amenaza contra el software encargado de estas tareas.

c) Catástrofes

Aunque veremos este tipo de amenazas más en profundidad en el apartado de Seguridad Física, creo que hay que mencionarlo en este repaso para hacernos una idea general de las amenazas hacia la entidad de un modo global.

Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales: simplemente por su ubicación geográfica, a nadie se le escapa que la probabilidad de sufrir un terremoto o una inundación que afecte a la entidad en una gran ciudad como Madrid, Valencia o Barcelona, es relativamente baja, al menos en comparación con el riesgo de sufrir un intento de acceso por parte de un pirata o una infección por virus. Sin embargo, el hecho de que las catástrofes sean amenazas poco probables no implica que contra ellas no se tomen unas medidas básicas, ya que si se produjeran generarían los mayores daños.

Un subgrupo de las catástrofes es el denominado de **riesgos poco probables**. Obviamente se denomina así al conjunto de riesgos que, aunque existen, la posibilidad de que se produzcan es tan baja (menor incluso que la del resto de catástrofes) que nadie toma, o nadie puede tomar, medidas contra ellos. Ejemplos habituales de riesgos poco probables son un ataque nuclear contra la entidad, el impacto de un satélite contra la sala de operaciones, o la abducción de un operador por una nave extraterrestre. Nada nos asegura que este tipo de catástrofes no vaya a ocurrir, pero la probabilidad es tan baja y los sistemas de prevención tan costosos que no vale la pena tomar medidas contra ellas.

Como ejemplos de catástrofes hablaremos de terremotos, inundaciones, incendios, humo o atentados de baja magnitud (más comunes de lo que podamos pensar).

1.5 - ¿Cómo nos podemos proteger?

Hasta ahora hemos hablado de los aspectos que engloba la seguridad informática, de los elementos a proteger, de los tipos de amenazas que contra ellos se presentan y del origen de tales amenazas; parece claro que, para completar nuestra visión de la seguridad, hemos de hablar de las formas de protección de nuestros sistemas. Cuando hayamos completado este punto, habremos presentado a grandes rasgos los aspectos básicos de la seguridad informática.

Para proteger nuestro sistema hemos de realizar un análisis de las amenazas potenciales que puede sufrir, las pérdidas que podrían generar, y la probabilidad de su ocurrencia; a partir de este análisis hemos de diseñar una política de seguridad que defina responsabilidades y reglas a seguir para **evitar** tales amenazas o **minimizar** sus efectos en caso de que se produzcan. A las medidas utilizadas para implementar esta política de seguridad se les denomina **medidas de seguridad**; su propósito es **disminuir** los riesgos (amenazas, vulnerabilidades, etc.) asociados a un activo en un momento y espacio concreto. No se habla de eliminar el riesgo, ya que siempre existirá un riesgo residual.

Podemos clasificar las medidas de seguridad en base a dos taxonomías:

a) Según su forma de actuación

Es la manera más común para clasificar las medidas de seguridad y se divide en cuatro grandes subgrupos. Vamos a ver cada uno de ellos y, para que quede más claro, un ejemplo de cada uno ante un posible incendio.

i) Prevención

Son aquellos que evitan que una amenaza se materialice. Aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad. Los ataques a la confidencialidad solo pueden protegerse mediante medidas de prevención. En el caso del incendio, un ejemplo sería instalar muebles ignífugos.

ii) Detección

Por medidas de detección se conoce a aquellas que se utilizan para detectar y avisar violaciones de la seguridad o intentos de violación que se están produciendo. Por ejemplo los sistemas de detección (no extinción) de incendios, como sensores de humo o de calor.

iii) Corrección

Las medidas de corrección son aquellas que corrigen o eliminan las violaciones de seguridad una vez que se han producido. Por ejemplo extintores o los sistemas de extinción de incendios.

iv) Recuperación

Son aquellas que se aplican cuando una violación del sistema se ha consumado, para retornar a éste a su estado anterior. Por ejemplo las primas de los seguros o las copias backup de los datos.

v) Análisis forense
Es un subgrupo de la recuperación, cuyo objetivo no es simplemente retornar el sistema al estado anterior al ataque, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema, las debilidades de la seguridad, etc. De esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de nuestra red. En el caso del incendio consistiría en ver como se ha producido, los activos afectados, como se ha sofocado, etc.

Parece claro que, aunque los cuatro tipos de medidas son importantes para la seguridad de nuestro sistema, hemos de enfatizar en el uso de medidas de prevención y de detección. La máxima popular "más vale prevenir que curar" se puede aplicar a la seguridad informática: para nosotros, evitar un ataque, detectar un intento de violación, o detectar una violación exitosa inmediatamente después de que ocurra es mucho más productivo y menos comprometedor para el sistema que restaurar el estado tras una penetración de la máquina. Es más, si consiguiéramos un sistema sin vulnerabilidades y cuya política de seguridad se implementara mediante medidas de prevención de una forma completa, no necesitaríamos mecanismos de detección o recuperación. Aunque esto es imposible de conseguir en la práctica, será en los mecanismos de detección, y sobre todo en los de prevención, en los que la entidad ha de hacer mayor hincapié.

b) Según su naturaleza

Esta clasificación es menos común, pero también es interesante.

i) Legales
Son las adoptadas por los poderes legislativos. Tratan de proteger la información como un bien específico, atendiendo a sus peculiaridades mediante sanciones. Vamos a ver algunas:

i.i) LOPD: La Ley Orgánica 15/1999, de 13/XII, de Protección de Datos de Carácter Personal (LOPD), y el R.D. 994/1999, de 11/VI, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal (Reglamento), son las dos disposiciones básicas de obligado cumplimiento para todas las empresas y profesionales que, en el desarrollo de su actividad, traten datos de carácter personal (además de otras normas complementarias de índole más sectorial).

i.ii) LPI: Ley de Protección Intelectual. Trata, entre otras cosas, la protección del software.

i.iii) Código Penal: Recoge y trata el delito informático.

i.iv) Ley de Firma Electrónica: Es un documento que expende la Fábrica Nacional de Moneda y Timbre. El sistema de certificación de firma electrónica establecido por la FNMT-RCM es un intermediario transparente al ciudadano, de fácil uso, que ofrece alta

disponibilidad y gran capacidad de acceso concurrente para los usuarios de la red. Este sistema ya está operativo con diversas aplicaciones en funcionamiento y numerosos organismos en fase de incorporación al sistema.

Los certificados emitidos por la FNMT-RCM son de uso general y por lo tanto universales, es decir, cada ciudadano puede comunicarse con las diferentes administraciones con un único certificado.

i.v) LSSI: Ley de servicios de la sociedad de la información y de comercio electrónico. Se pretende facilitar el desarrollo del comercio electrónico sin mermar ninguna de las garantías con las que cuentan los usuarios en sus relaciones de comercio convencional.

ii) Administrativo / Organizativas
Pretenden gestionar la seguridad pero no son medidas técnicas. Son muy importantes ya que dictan la seguridad de la entidad.

ii.i) Clasificación de la información. Pretende saber que información es más valiosa para la entidad y cual menos. Existen muchos factores que puedan hacer que cierta información sea más o menos importante. Por ejemplo, el tiempo que ha llevado confeccionarla, los datos técnicos de la entidad, datos personales, etc.

ii.ii) Asignación de responsabilidad. Es importante que toda persona que maneja información sepa cuales son sus responsabilidades. Esto es, no dañarla, no revelarla, etc.

ii.iii) Establecimiento de la función de seguridad. Es decir, que exista un responsable de la seguridad de la información, distinto de la seguridad corporativa, ya que este no tiene porqué conocer los métodos de seguridad de la información.

ii.iv) Formación y Sensibilidad. Tenemos que concienciar de que la información es muy valiosa para cualquier entidad y que por tanto es importante mantener unas pautas de seguridad, como no dejar el terminal encendido e irse, anotar contraseñas en el propio terminal, etc.

iii) Físicas
Vamos a ver todas estas medidas mucho más en profundidad, pero es necesario reflejarlas en este apartado. Tratan de compensar las amenazas de tipo físico. Afectan a los sistemas de información y su entorno, imprescindible para su correcto funcionamiento. Por ejemplo su ubicación, los canales de redes, los sistemas de alimentación, etc.

iv) Técnicas
Son aquellas que actúan desde dentro del sistema de información, adaptadas al software y hardware.

iv.i) Identificación y Autenticación. Suele ser la primera medida que uno se encuentra al acceder a un sistema de información, la más empleada es nombre de usuario y contraseña, aunque la autenticación puede ser:

- Por algo que se tiene, como una llave o una tarjeta.
- Por algo que se sabe, como una clave o contraseña.
- Por algo que se es (biometría), como la huella digital, la voz o el iris.

iv.ii) Control de accesos a recursos. Se encarga de controlar el permiso de acceso a cada recurso del sistema y actúa cuando el sistema ya ha permitido la entrada.

iv.iii) Control de flujo de la información. Es la más novedosa y sofisticada, por lo que aún no está presente en todos los sistemas de información. Consiste en controlar lo que hace el usuario con la información a la que accede.

iv.iv) Confidencialidad. Trata de evitar que se descubra información secreta. Nadie puede acceder a información que no debe acceder.

iv.v) Integridad. Consiste en evitar que la información sea alterada.

iv.vi) No repudio. Evita que el emisor de una información pueda rechazar el hecho de serlo, es decir, que no se responsabilice de ella.

iv.vii) Notariado. Consiste en que una institución (persona jurídica) de fe de elementos como las claves públicas de los usuarios. También son conocidos como notarios electrónicos.

iv.iix) Auditoria. Es un registro en el que se almacenan todas las acciones de los usuarios. Es una medida preventiva y disuasoria.

Esquema 1.2

1.6 - Mecanismos de seguridad

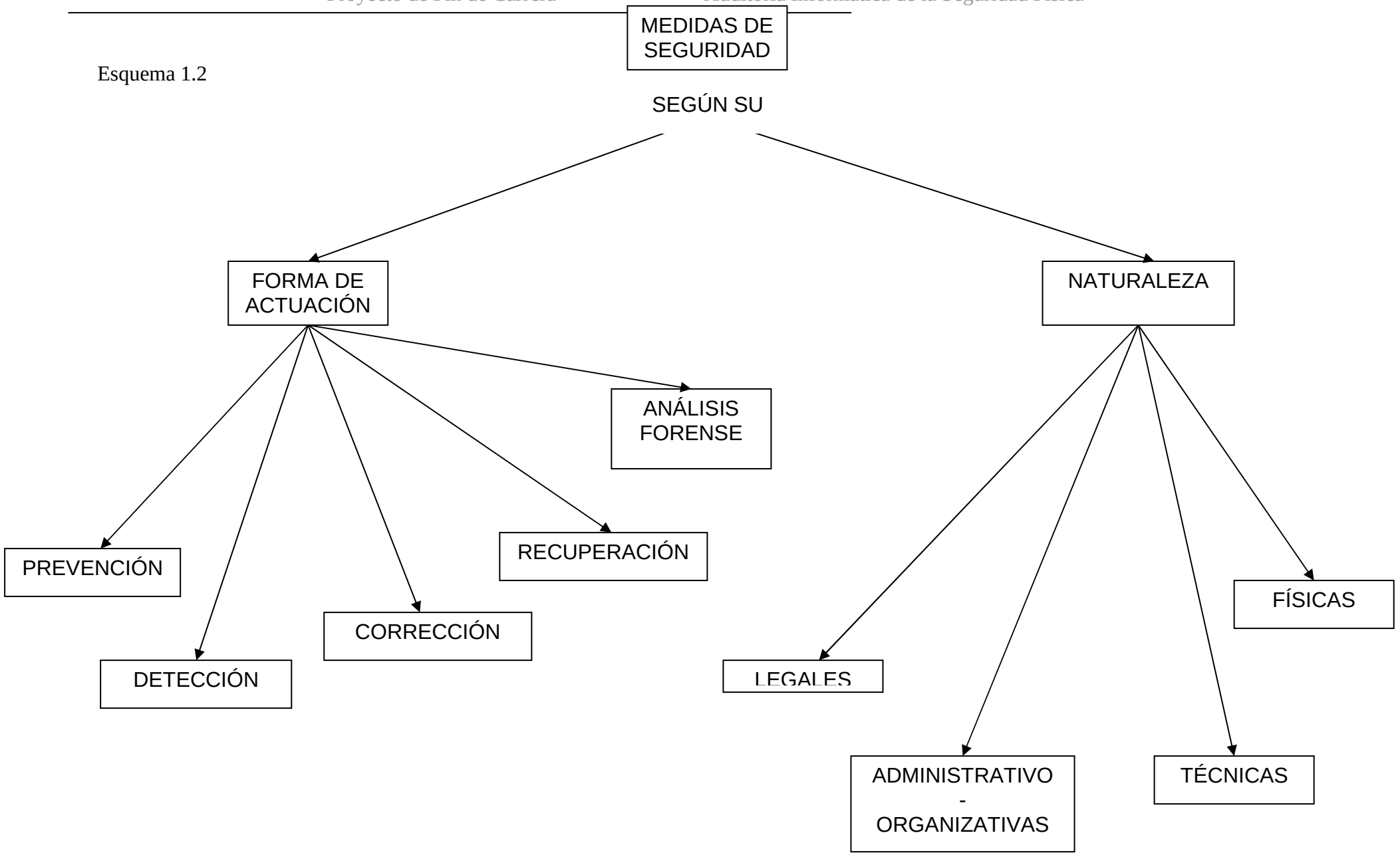
Para poder aplicar todas las medidas de seguridad y protección expuestas anteriormente se han de implementar una serie de mecanismos de seguridad. Estos mecanismos se implementan con software, hardware u otros dispositivos y reciben en ocasiones los mismos nombres que las medidas de seguridad. Los tipos de mecanismos son:

a) Mecanismos de autenticación e identificación

Estos mecanismos hacen posible identificar entidades del sistema de una forma única, y posteriormente, una vez identificadas, autenticarlas (comprobar que la entidad es quién dice ser). Son los mecanismos más importantes en cualquier sistema, ya que forman la base de otros mecanismos que basan su funcionamiento en la identidad de las entidades que acceden a un objeto.

Un grupo especialmente importante de estos mecanismos son los denominados Sistemas de Autenticación de Usuarios, ya que es con lo primero que se van a encontrar los usuarios del sistema y la primera traba para los posibles atacantes.

Esquema 1.2


MEDIDAS DE SEGURIDAD
SEGÚN SU
FORMA DE ACTUACIÓN
NATURALEZA
ANÁLISIS FORENSE
PREVENCIÓN
RECUPERACIÓN
CORRECCIÓN
DETECCIÓN
FÍSICAS
LEGALES
ADMINISTRATIVO - ORGANIZATIVAS
TÉCNICAS

b) Mecanismos de control de acceso

Cualquier objeto del sistema ha de estar protegido mediante mecanismos de control de acceso, que controlan todos los tipos de acceso sobre el objeto por parte de cualquier entidad del sistema.

c) Mecanismos de separación

Cualquier sistema con diferentes niveles de seguridad ha de implementar mecanismos que permitan separar los objetos dentro de cada nivel, evitando el flujo de información entre objetos y entidades de diferentes niveles siempre que no exista una autorización expresa del mecanismo de control de acceso. Los mecanismos de separación se dividen en cinco grandes grupos, en función de como separan a los objetos: separación física, temporal, lógica, criptográfica y fragmentación.

d) Mecanismos de cifrado de datos

Son mecanismos básicos para la confidencialidad y la integridad. Existen múltiples técnicas de cifrado y en ellas se va a basar gran parte de la seguridad de los datos de la entidad, ya que, como hemos comentado antes, los ataques a la confidencialidad solo pueden ser protegidos por medidas de prevención, y el cifrado es un mecanismo utilizado en medidas de prevención.

e) Mecanismos de firma digital

Es un mecanismo que emplean las medidas de no repudio, verificando que una persona no pueda negar lo que ha hecho. La firma digital se encuentra incorporada en multitud de aplicaciones, tales como la presentación de la declaración del IRPF, la descarga de *plug-ins* auto instalables en los navegadores, el acceso seguro a servidores WEB, el pago mediante tarjeta de crédito, etc. Sin embargo, la aplicación más popular e intuitiva de la firma digital es el correo electrónico.

f) Mecanismos de funciones resumen

Este mecanismo proporciona integridad a los datos. Consiste en la proyección de un conjunto, esto es, partiendo de un conjunto con un número elevado elementos (los datos) se llega mediante la función resumen a un conjunto con un número mucho menor de elementos (resumen). En criptografía ha de cumplir los siguientes requisitos:

i) La entrada puede ser de un tamaño indeterminado.
ii) La salida es de un tamaño fijo, varios órdenes de magnitud menor que la entrada
iii) Calcular la función resumen es computacionalmente barato.
iv) Es irreversible, esto es, con el resumen no se puede obtener la entrada.
v) No presenta colisiones, esto es, a entradas distintas le corresponden resúmenes distintos.

g) Mecanismos de registros de auditoria

Se emplean en las medidas de auditoria. Son ficheros en los que se almacena información sobre quién y qué se hace. Además existen programas que interactúan con estos ficheros pueden decirnos, incluso en tiempo real, si existe algún problema en nuestro sistema, si alguien ha hecho algo que no debía o incluso si se ha equivocado más de dos veces al introducir su contraseña.

2 - SEGURIDAD FÍSICA

2.1 - INTRODUCCION

2.1.1 - ¿Qué entendemos por Seguridad Física?

Por lo general, cuando se habla de seguridad informática siempre se piensa en errores de software, virus, intrusos de red, etc. En definitiva, pensamos en software. La realidad es que la seguridad informática también implica otro aspecto muy importante y que generalmente permanece desatendido. Se trata de la Seguridad Física de un sistema.

¿De qué sirve que nadie pueda acceder de forma autorizada a los recursos lógicos del sistema, si cualquiera puede entrar por la puerta y llevarse el equipo debajo del brazo?

Por lo tanto, se deben tomar medidas en lo que respecta a la seguridad física del sistema, y por supuesto, cuando se definen dichas medidas hay que tener en cuenta a las personas que trabajan con los equipos informáticos.

Una definición formal podría ser esta.

> *"… la seguridad física de los sistemas informáticos consiste en la aplicación de barreras **físicas** y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial"*
> Sue Berg et al. Glossary of Computer Security Terms

Más claramente, por Seguridad Física podemos entender *todos aquellos mecanismos destinados a proteger **físicamente** cualquier recurso del sistema. Estos recursos son desde un simple teclado hasta una cinta de backup con toda la información de nuestra entidad, pasando por la propia CPU de la máquina, el cableado eléctrico o el edificio al completo.*

En esta parte del trabajo vamos a ver cuales son los factores que pueden amenazar la Seguridad Física de nuestra entidad, o más concretamente, nuestra información. Así mismo, veremos cuales son las causas y las posibles soluciones a estos factores o amenazas. Se quiere decir con esto que se va a dar una visión general, aplicando soluciones concretas y métodos en la parte de *auditoría de de la seguridad física*, donde seguiremos normas y estándares.

Existen también normas y leyes de obligado cumplimiento en lo que a instalaciones se refiere, tales como las aplicables a sanidad o personal. En este trabajo vamos a dejar éstas de lado para centraros en las que incumban a la información, los datos o los sistemas informáticos.

2.1.2 - Factores a tener en cuenta

a) Seguridad Física olvidada

Desgraciadamente, la seguridad física es un aspecto olvidado con demasiada frecuencia a la hora de hablar de seguridad informática en general; en muchas entidades se suelen tomar medidas para prevenir o detectar accesos no autorizados a la red o a datos almacenados en servidores, pero rara vez para prevenir la acción de un atacante que intenta acceder físicamente a la sala donde se encuentran éstos o a al armario donde se guardan las cintas con los backups(8). Esto motiva que en determinadas situaciones un atacante se decline por aprovechar vulnerabilidades físicas en lugar de lógicas, ya que posiblemente le sea más fácil robar una cinta con una imagen completa del sistema que intentar acceder a él remotamente mediante fallos en el software.

(8) Copia de seguridad o copia de respaldo. Consiste en hacer una copia de la información sensible referida a un sistema. La copia se puede realizar en cualquier medio, incluso otro PC o servidor. De esta manera, en caso de perdida de los datos originales, se podrá recurrir a la copia guardada en lugar seguro.

Hemos de ser conscientes de que la seguridad física es demasiado importante como para ignorarla: un ladrón que roba un ordenador para venderlo, un incendio o un pirata que accede sin problemas a la sala de operaciones nos pueden hacer mucho más daño que un intruso que intenta conectar remotamente con una máquina no autorizada. No importa que utilicemos los más avanzados medios de cifrado para conectar a nuestros servidores, ni que hayamos definido una política de *firewall*(9) muy restrictiva, si no tenemos en cuenta factores físicos, estos esfuerzos para proteger nuestra información no van a servir de nada.

(9) Cortafuegos. Es un elemento de hardware o software utilizado en una red de computadoras para prevenir algunos tipos de comunicaciones prohibidas por las políticas de red, las cuales se fundamentan en las necesidades del usuario.

b) Efecto disuasorio

En el caso de organismos con requerimientos de seguridad medios, unas medidas de seguridad físicas ejercen un efecto disuasorio sobre la mayoría de piratas: como casi todos los atacantes de los equipos de estos entornos son casuales (esto es, no tienen interés específico sobre nuestros equipos, sino sobre cualquier equipo), si notan a través de medidas físicas que nuestra organización está preocupada por la seguridad probablemente abandonarán el ataque para lanzarlo contra otra red menos protegida.

c) La Seguridad Física no es universal

Aparte de que cada entidad es diferente, y por lo tanto tendrá unas necesidades de seguridad distintas, hay que tener en cuenta múltiples factores, como son la zona geográfica, la orografía del terreno o la sociedad en la que se emplaza. Cada uno de estos factores, que veremos en profundidad más adelante, tiene unas peculiaridades concretas, por lo que no se pueden dar recomendaciones específicas sino pautas generales a tener en cuenta, que pueden variar desde el simple sentido común (como es

el cerrar con llave la sala de operaciones cuando salimos de ella) hasta medidas mucho más complejas, como la prevención de radiaciones electromagnéticas de los equipos o la utilización de sistemas antirrobo complejos.

d) Visión global y específica

Este punto es extremadamente importante ya que una acumulación de medidas de seguridad puntuales sobre un dispositivo o sistema concreto no nos proveerán de una seguridad física aceptable si no tenemos en cuenta el aspecto global del problema, como el entorno físico y social donde estas máquinas van a cumplir su función.

Es un error muy común en los estudios de seguridad física el centrarse en el hardware específicamente, asegurando las máquinas y dispositivos de red, pero descuidando el entorno donde estas máquinas han de trabajar, que es tan importante como el mismo hardware que ha de soportar las aplicaciones. Trataremos por tanto de ir desde lo global a lo específico, desde el edificio donde se alojará el hardware y el suministro de energía o el control de accesos, hasta lo más específico del hardware que ha de soportar nuestras aplicaciones, llegando incluso a los ordenadores y sus componentes o al acceso físico a las bocas de red de los concentradores que proporcionan acceso a nuestra red local.

2.2 - EL ENTORNO DEL EDIFICIO

2.2.1 - Introducción

Puesto que vamos a analizar el sistema desde lo global hasta lo específico, lo primero que tenemos que analizar en el estudio de la Seguridad Física es el entorno del edificio donde se éste encuentre. Ya sea todo el edificio de nuestra propiedad o simplemente unas oficinas dentro de una edificación compartida, tendremos que tener presentes los factores externos que nos puedan afectar. A estos factores externos se les denomina **factores inherentes a la localidad** y los podemos englobar en cuatro categorías: **naturales**, **no naturales**, **de servicios** y **sociales**. Veremos estos factores en profundidad a continuación.

2.2.2 - Factores inherentes a la localidad

Hay que dejar claro que estos factores afectan o pueden afectar directamente a nuestros sistemas, por lo que veremos en cada caso las pautas que debemos seguir, incluso en el entorno del hardware, para estar protegidos frente a estas amenazas. Precisamente, el enfoque global que hacemos nos va a permitir conocer las deficiencias o las medidas de seguridad concretas que debemos adoptar para hacer frente a problemas mucho más generales. Veremos cada una de las pautas que debemos seguir para hacer frente a estos grandes problemas mucho más en concreto cuando hablemos del lugar donde se deben desarrollar, como **el entorno físico de hardware** o **el interior del edificio.**

Sin embargo, en gran medida, la protección de nuestras instalaciones ante las amenazas que provienen del entorno será llevado a cabo por entidades externas, tales como el ayuntamiento local que se encargue del alcantarillado zonal o el servicio de bomberos, en caso de un incendio cercano. Pero como afectados directos debemos velar por que se cumplan los requisitos que nos garanticen seguridad.

a) Naturales

Los factores naturales son los que se producen sin que intervenga la mano del hombre, tales como las temperaturas extremas, los seísmos, la humedad o los terremotos, llegando a denominarse **desastres naturales** si sobrepasan un cierto nivel de intensidad. El tipo de factor natural y la frecuencia con que se produzca depende en gran medida de la zona geográfica en la que nos encontremos, por lo que aunque sus efectos pueden suponer una gran amenaza para la entidad, podemos estar preparados para hacerles frente, ya que podemos saber con cierta certeza si se van a producir o no.

Aunque en algunas zonas geográficas la probabilidad de que se produzca una de estas catástrofes es casi nula, se tiene que realizar un estudio para conocer en que medida es dicha zona propensa a sufrir alguno de éstas. Veremos, en cualquier caso, algunas sencillas pautas que nos pueden evitar imprevistos fácilmente controlables. Los factores naturales más comunes son los siguientes.

i) Terremotos

Los terremotos o seísmos son sacudidas del terreno ocasionadas por fuerzas en el interior de la corteza terrestre. Éstas pueden tener distinta intensidad y van desde unos temblores que apenas se aprecian hasta movimientos tan fuertes que son capaces de partir carreteras, tirar edificios e incluso montañas.

Por tanto, las medidas que se han de tomar ante esta amenaza dependen de la probabilidad de que se produzca y de la intensidad con la que lo haga. En Japón, por ejemplo, donde la probabilidad de que se produzca un terremoto de gran intensidad es muy alta, se están construyendo edificios con un enorme péndulo a modo de contrapeso, capaces de resistir una gran sacudida.

En la Península Ibérica estas medidas carecen de sentido, ya que la probabilidad de que tenga lugar un gran terremoto es casi nula, solamente en Andalucía, Cataluña, País Vasco y Aragón existe un cierto riesgo de que se dé este fenómeno natural, pero siempre con una intensidad muy baja.

Las medidas de precaución que se deben tomar son las siguientes.

i.i) Evitar situar los equipos o material delicado en superficies altas.
i.ii) No colocar objetos pesados por encima de este material delicado.
i.iii) No ubicar equipos cerca de las ventanas, ni en general nada que pudiera caer por éstas.
i.iv) Plantearse la posibilidad de fijar los equipos a la superficie en la que se encuentran.

ii) Tormentas eléctricas

Las tormentas eléctricas se originan cuando en una tormenta convencional se dan unas ciertas condiciones, tales como la carga eléctrica de las nubes y la del terreno sobre el que están, el tipo y concentración de precipitación o la ionización del aire. Estas condiciones se dan normalmente en épocas calurosas y secas, por lo que en verano es muy normal que se dé éste fenómeno en toda la extensión de la Península Ibérica.

Cuando hablamos de tormenta eléctricas, debemos entender que el factor que mayor riesgo entraña para nuestra entidad es que se establezca el rayo eléctrico. Esto se produce cuando se alcanza la tensión de ruptura del aire, es decir, cuando el aire se convierte en un medio conductor de la electricidad.

La caída de un rayo descontrolado en la superficie de la tierra tiene una gran probabilidad de provocar un incendio, dada la gran intensidad eléctrica con la que cuenta. Para controlarlo la única manera posible es la de emplear pararrayos, evitando que éste caiga sobre árboles o antenas. Vemos por tanto que una tormenta eléctrica entraña un riesgo de incendio.

Además, los sistemas electrónicos de que disponga nuestra entidad, como veremos más adelante, son muy vulnerables ante una descarga de electricidad estática, por lo que parece evidente que la caída de un rayo, que podríamos decir que es la descarga de electricidad estática más potente que podemos encontrar, puede dejarlos del todo inservibles.

Las medidas de seguridad que se deben tomar son las siguientes.

ii.i) Es imprescindible que en el propio edificio en el que nos encontramos o en los alrededores cercanos a éste esté instalado un pararrayos. De no ser así, o como medida de precaución añadida, deberemos proceder a la instalación de uno propio en nuestras instalaciones. Para ello deberemos contratar a una empresa especializada y verificar que ésta cumple con lo especificado en el "REAL DECRETO 1428/1986 - Homologación de pararrayos".

ii.ii) Como veremos más adelante, se deben de proteger los equipos con sistemas de regulación de corriente, para evitar que una subida de tensión los dañe. Los equipos que no estén protegidos por este sistema es conveniente que se desconecten durante una tormenta eléctrica fuerte.

ii.iii) Se debe evitar colocar equipos eléctricos o medios de almacenamiento ópticos cerca de las estructuras metálicas para evitar posibles descargas de electricidad estática.

iii) Temperatura

La temperatura es un factor muy a tener en cuenta en los sistemas informáticos. Es obvio que dependiendo de la zona o el período del año en el que nos encontremos la temperatura ambiente variará enormemente. Además a este factor le influye mucho la humedad ambiental, que veremos a continuación.

Las temperaturas bajas o, incluso, excesivamente bajas no deben preocuparnos, ya que los sistemas eléctricos pueden funcionar a una temperatura ambiente varios grados por debajo de cero, y ciertamente, nunca llegaremos a esa situación en el interior de nuestro edificio. Solo cabe mencionar que ante una temperatura externa muy baja tendemos a poner la calefacción interior muy alta, incluso más de lo adecuado, por lo que podríamos hacer que la temperatura en el interior de nuestro edificio subiera en exceso.

Por el contrario, una temperatura alta si afecta muy negativamente a nuestros sistemas, y de todos es sabido que en periodos de verano se alcanzan temperaturas muy elevadas en toda la Península Ibérica, y más aún en el interior de las grandes ciudades.

Aunque pudiera parecer un factor poco importante, está demostrado que a mayor temperatura menor es el tiempo entre fallos de un dispositivo electrónico, incluyendo ordenadores, servidores y cualquiera que genere por si mismo calor, ya que a una mayor temperatura ambiente, más le cuesta disipar y desprenderse de ese calor.

Aunque veremos mucho más en profundidad este factor en el entorno físico del hardware y en el propio hardware, vamos a ver unas pequeñas pautas que se deben seguir.

iii.i) Disponer de climatizadores automáticos para todo el edificio y especialmente para las salas donde se disponga de material electrónico, equipos, dispositivos de almacenamiento, etc.

iii.ii) Conocer cual es el rango de tolerancia de temperatura de todos los sistemas sensibles a ésta. Instalarlos y configurarlos adecuadamente.

iii.iii) Revisar periódicamente que todos los sistemas de refrigeración de los sistemas, tales como ventiladores o disipadores, funcionan correctamente. A ser posible monitorizar todos estos sistemas para evitar que en un fallo de ventilación pueda dañar permanentemente un dispositivo.

iv) Humedad

Se entiende por humedad la cantidad de vapor de agua presente en el aire. Se puede expresar de forma absoluta mediante la humedad absoluta, o de forma relativa mediante la humedad relativa o el grado de humedad. La manera en que normalmente se maneja este factor es mediante la humedad relativa.

La humedad relativa depende en gran medida de la temperatura ambiente, no se debe olvidar nunca este detalle, ya que si la temperatura es baja, la humedad relativa ha de ser menor que si la temperatura fuese alta. Además varía mucho de unas zonas a otras, dependiendo sobre todo de la vegetación de la zona, ya que ésta aumenta considerablemente el nivel de humedad. También en las zonas de costa la humedad es más alta que en las de interior.

Por lo general, se considera que la humedad es un enemigo de los equipos, sin embargo, como ya hemos mencionado, un ambiente seco, o lo que es lo mismo, con poca

humedad, es favorable para que se produzcan descargas de electricidad estática. Por lo tanto, se deberá tener un nivel de humedad adecuado, normalmente entre el 40% y el 70%.

Para evitar que la humedad se convierta en un problema, las pautas que se deben seguir son las siguientes.

iv.i) Es recomendable conocer cuál es la tolerancia a la humedad de todos nuestros sistemas, sobre todo de los más críticos. Normalmente en las especificaciones técnicas de éstos lo podremos encontrar fácilmente.

iv.ii) Se debe conocer cuál es la humedad relativa ambiente, sobre todo de las zonas donde se encuentren nuestros equipos eléctricos más sensibles a ésta. Para ello se pueden instalar sensores. Como veremos más adelante, existen sistemas independientes o incorporados en climatizadores.

iv.iii) Para variar el nivel de humedad relativa podemos emplear dos sistemas: los deshumidificadores para reducir el nivel de humedad y los humidificadores, para incrementarlo.

v) Lluvias

Uno de los elementos que más pueden dañar todos nuestros sistemas eléctricos, dispositivos de almacenamiento o archivos es el agua. Ésta puede llegar hasta nuestras instalaciones por diversos motivos, pero ahora nos centraremos en los factores naturales que pueden provocar una inundación.

El más obvio y la principal causa de las inundaciones fluviales suelen ser las lluvias intensas, que dependiendo de la región se producirán bajo diversos factores meteorológicos. Cuando se producen estas lluvias puede que las calles se conviertan en improvisados caudales para el agua, por lo que ésta se puede llegar a filtrar hasta nuestras instalaciones.

Aunque en principio la lluvia sea el causante de las inundaciones, lo normal es que se de algún otro condicionante para que éstas se produzcan, ya que el nivel de agua sólo por la lluvia no suele subir demasiado deprisa. Los factores que pueden provocar una inundación son los siguientes.

v.i.i) Desbordamiento de ríos. Normalmente debido a lluvias intensas, se incrementa el caudal de éste. Cuando esto sucede se vierte de golpe mucho agua y suele provocar inundaciones.

v.i.ii) Avalanchas de agua. Suele ocurrir en zonas de montaña, ya que se han desviado multitud de caudales naturales de agua y ésta tiende a fluir por su sitio natural.

v.i.iii) Zonas donde el nivel del suelo es más bajo que el de las zonas colindantes. Esto provoca que el agua se concentre en estas zonas más bajas.

Se debe tener especial cuidado con las inundaciones si nos encontramos en una zona de alto riesgo de que se produzcan aunque podemos ser más relajados si nuestras instalaciones se encuentran a cierta altura del nivel del suelo. En cualquier caso, las pautas que debemos seguir para evitar una inundación son las siguientes.

v.ii.i) No ubicar nuestras instalaciones en caudales naturales de agua, aunque éstos estén secos, ante una situación de fuertes lluvias podrían convertirse en voluminosos ríos.

v.ii.ii) Evitar que nuestras instalaciones estén cerca de ríos o lagos, evitar también que estén en zonas donde acaba una pendiente del terreno o en zonas más bajas que el perímetro de ésta.

v.ii.iii) No ubicar el centro computacional o elementos críticos en sótanos o plantas bajas y nunca colocar estos dispositivos en el suelo.

v.ii.iv) Disponer de sensores de agua y en caso de que la zona en la que nos encontremos sea propensa a que ocurran inundaciones (lo veremos más adelante), disponer de bombas extractoras de agua.

v.ii.v) Verificar que el alcantarillado cercano a la entidad se encuentra limpio, desatascado y operativo al cien por cien.

v.ii.v) Verificar que nuestras puertas y ventanas no filtran el agua. Además, las ventanas deben tener un cierre hermético.

vi) Otros factores

Los factores que vamos a ver a continuación van a afectar de manera insignificante o nula por completo a nuestra organización, no obstante, creo que debemos mencionarlos para tener conocimiento de éstos.

vi.i) Vientos. Normalmente en la Península Ibérica los vientos no alcanzan velocidades preocupantes, y menos en el interior de las ciudades, ya que los propios edificios se protegen unos a otros. Solo en las Islas Canarias se pueden llegar a registrar vientos con velocidades por encima de los 100 Km. por hora con una cierta normalidad. Aún así las edificaciones no se suelen ver afectadas por este factor. Como más daño nos podrían causar es derribando árboles que a su vez afecten a líneas de comunicaciones o tendidos eléctricos.

vi.ii) Granizo. El granizo es un tipo de precipitación que consiste en partículas irregulares de hielo. El granizo se produce en tormentas intensas en las que se producen gotas de agua sobreenfriadas, líquidas pero a temperaturas por debajo de su punto normal de fusión, y ocurre tanto en verano como en invierno a lo largo de toda la Península Ibérica. Los mayores daños que pueden causar son la rotura de cristales o persianas y, en el peor de los casos, sistemas vulnerables que se encuentren en el exterior, como los ventiladores de los sistemas de climatización o las cámaras de vigilancia.

vi.iii) Radiaciones Solares. En principio, las radiaciones solares no plantean un problema en el interior de las instalaciones, pero hay que tener en cuenta que muchos dispositivos electrónicos o de almacenamiento pueden sufrir daños si están expuestos a éstas durante un largo periodo de tiempo.

b) No naturales

Son los que son provocados por el entorno pero no tienen un origen natural, tales como el polvo que puede producir una empresa, por ejemplo de cementos, el riesgo de incendio que produce una empresa pirotécnica cercana, las vibraciones que origina un tren o las interferencias que pueda causar una antena de repetición.

A diferencia de los naturales, los no naturales no siguen ninguna pauta para producirse, podremos hacer un estudio de las actividades que se realizan en el entorno del edificio pero estas pueden cambiar en cualquier momento.

Dado que éstas nos afectan directamente, deberemos velar por que las entidades que operan a nuestro alrededor lo hagan siguiendo unas pautas de seguridad. Por ejemplo, si una empresa maderera cercana almacena restos en el patio y pensamos que puede provocar un incendio, deberemos avisar a las autoridades para que actúen en consecuencia.

Los elementos de esta índole más comunes que pueden afectar a nuestros sistemas son los siguientes.

i) Vibraciones

Las vibraciones pueden estar originadas por múltiples motivos, incluso por algunos procedentes del interior de nuestras propias instalaciones, los cuales veremos más adelante. Principalmente las vibraciones son originadas por vehículos pesados, tales como grandes excavadoras trabajando en una cantera, la red de metro o trenes.

Es difícil que las vibraciones alcancen un nivel perceptible para las personas, no obstante tras un largo periodo de tiempo pueden dañar gravemente nuestros sistemas, sobre todo los discos duros, ya que la cabeza lectora se encuentra calibrada con una precisión de micras sobre la superficie magnética. Por lo tanto es importante evitar que las vibraciones afecten a nuestros sistemas.

Para ello debemos realizar las siguientes acciones.

i.i) Colocar los equipos sensibles a las vibraciones lo más alejado de los elementos que las provoquen.

i.ii) Los dispositivos extremadamente sensibles, como discos duros, pueden ser aislados con gomas o capas de goma espuma que amortigüen las vibraciones.

ii) Polvo

Como ya hemos mencionado, una empresa que se dedica a remover el terreno, como una cantera o una productora de cementos, genera unas partículas de polvo que se quedan suspendidas en el aire. Estas partículas son altamente perjudiciales para nuestros sistemas. Al margen de que pueden ser conductoras de la electricidad y generar un cortocircuito en alguno de nuestros dispositivos, se van almacenando hasta, literalmente, obstruir por completo los sistemas de ventilación.

Para evitar que esto ocurra lo que debemos hacer es lo siguiente.

ii.i) Si tenemos instalados climatizadores o sistemas de ventilación, estos normalmente cuentan con filtros antipartículas, debemos limpiarlos regularmente y cambiarlos cuando sea necesario.

ii.ii) Si no tenemos instalados estos sistemas, lo que se debe hacer es colocar purificadores de aire.

ii.iii) A nivel de hardware, debemos instalar filtros en nuestras máquinas, limpiarlos y cambiarlos cada cierto tiempo.

ii.iv) Los equipos deben estar limpios, por lo que cada cierto tiempo es conveniente desmontarlos y limpiarlos.

ii.v) En ambientes donde existe gran cantidad de polvo difícil de controlar, no estará de más el uso de fundas o cubiertas para los teclados y los equipos que no se usen durante un largo periodo de tiempo.

iii) Incendios

Los incendios son una gran amenaza para cualquier entidad, tanto si se producen en el interior de la misma, lo cual veremos más adelante, como si se producen en las inmediaciones de ésta. Dada la importancia de esta amenaza dedicaremos un apartado para saber como prevenirla, detectarla y, llegado el caso, extinguirla.

En este punto solo cabe mencionar que las actividades que se desarrollan en las inmediaciones de nuestras instalaciones pueden tener un alto riesgo de sufrir un incendio, lo que nos afectaría directamente, ya que un incendio en un edificio contiguo o en una oficina cercana es muy probable que nos afectara. Cuantos más factores incrementen el riesgo de sufrir un incendio, más preparados debemos estar.

Las actividades que más riesgo entrañan son las que manejan material inflamable, como papel, madera, sustancias químicas o plásticos y derivados del petróleo. También las fábricas de material pirotécnico o explosivo tienen un alto riesgo de sufrir un incendio.

En principio lo único que podemos hacer es velar por que estas entidades no almacenen productos o sobrantes de manera descontrolada en los patios e incrementar nuestras medidas de prevención, detección y extinción de incendios.

iv) Interferencias

Podríamos definir una interferencia como cualquier proceso el cual altera, modifica o destruye una señal durante su trayecto entre el emisor y el receptor. Dichos procesos pueden tener su origen en antenas de radio, grandes motores, equipos eléctricos o líneas de eléctricas.

Normalmente diremos que las interferencias son las que se transmiten por el aire y el ruido eléctrico es el que se transmite por los cables. Generalmente las interferencias no suelen interferir en los equipos, no obstante, si notamos anomalías en éstos deberemos tener presente que puede que se deba a dicho fenómeno. Veremos más adelante como por medio de filtros podemos evitar el ruido eléctrico.

iv.i) Si existe un emisor de ondas que pudiera interferir en nuestros sistemas en las inmediaciones de nuestra entidad, lo que debemos hacer es colocar lo más alejado de éste todos los elementos susceptibles de sufrir algún daño o anomalía en su funcionamiento.

c) Servicios

Existen una serie de servicios que son necesarios para el funcionamiento de la entidad, por lo que este es un aspecto muy importante del entorno de ésta. Debemos cerciorarnos de que la zona cuente con dichos servicios, que se encuentren disponibles y operen eficientemente. Entre los factores a considerar tenemos las líneas de comunicación, la energía eléctrica, el drenaje, las facilidades de comunicación para los empleados, etc.

En este trabajo solo vamos a ver dos de estos servicios, los cuales son **los suministros de energía eléctrica del edificio** y **los enlaces de comunicaciones**. Los veremos en profundidad cuando analicemos *el edificio*. El resto no los vamos a estudiar.

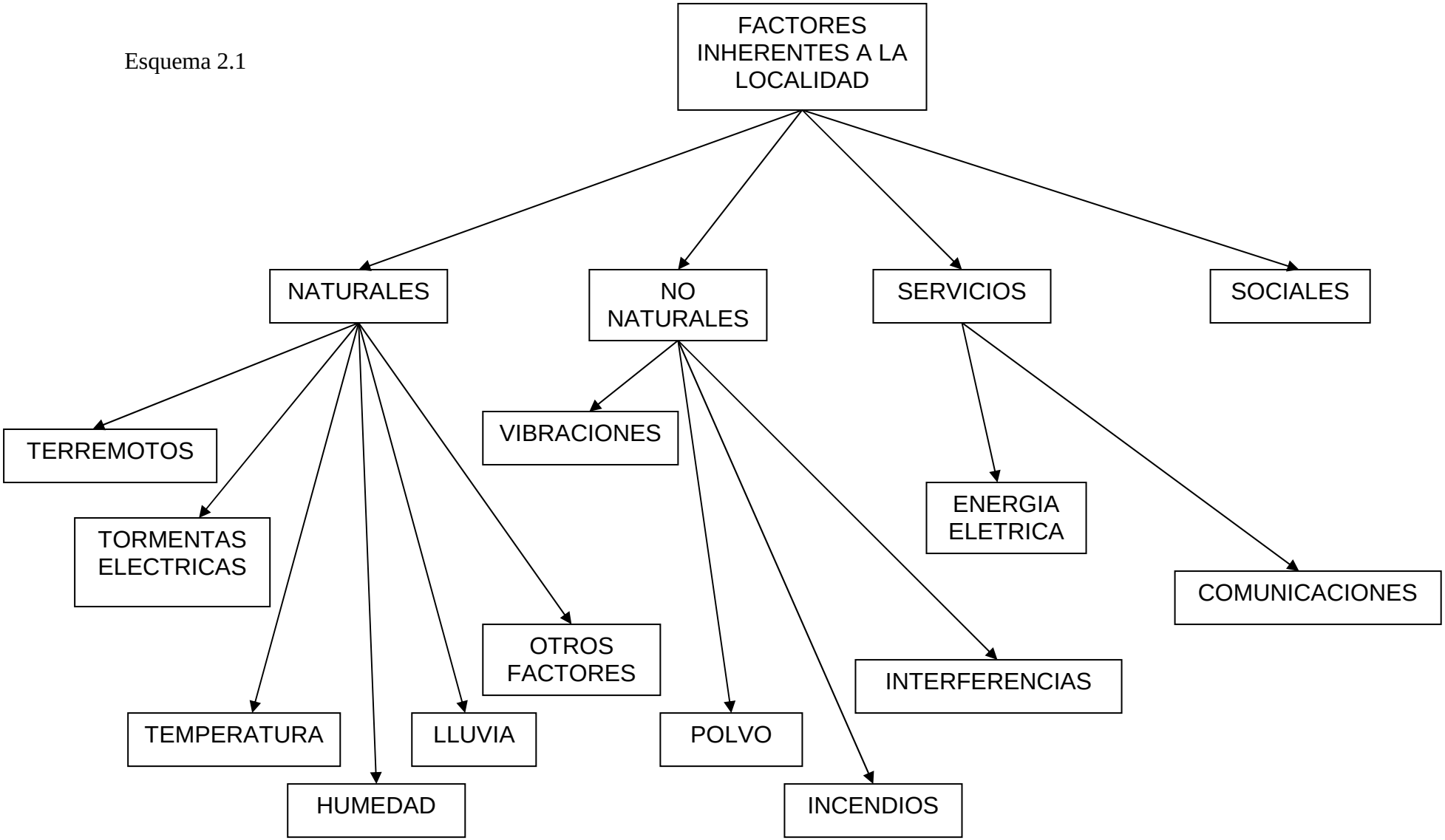
d) Social

Podemos hablar de dos cuestiones principales a la hora de estudiar este factor, el primero se basa en que sea una zona donde pueda encajar nuestra entidad o la actividad que vamos a desarrollar, por ejemplo, si montamos una central nuclear en un entorno urbano puede que no sea bien visto por el entorno social.

La otra cuestión de la que podemos hablar es que sea una zona tranquila, que no sea un lugar en el que sean frecuentes los actos vandálicos o los robos (tanto a la entidad como al personal de esta). Estos factores están relacionados, ya que uno puede dar lugar al otro. Es decir, si nos encontramos en lugar donde nuestra actividad no es bien vista, podemos sufrir ataques o sabotajes por gente que en principio no nos suponía este riesgo. Y al revés, si nuestra entidad es el blanco perfecto para ladrones o vándalos podemos centrar la atención del entorno en el que nos hemos asentado.

Esquema 2.1

Esquema 2.1


FACTORES INHERENTES A LA LOCALIDAD
NATURALES
NO NATURALES
SERVICIOS
SOCIALES
TERREMOTOS
TORMENTAS ELECTRICAS
TEMPERATURA
HUMEDAD
LLUVIA
OTROS FACTORES
VIBRACIONES
POLVO
INCENDIOS
INTERFERENCIAS
ENERGIA ELETRICA
COMUNICACIONES

2.3 - EL EDIFICIO

Como hemos comentado anteriormente, vamos a ir viendo los factores de la Seguridad Física desde lo más global hasta lo más específico, por lo que tras analizar el entorno del edificio, lo siguiente es analizar el propio edificio, que es lo que rodea a nuestro centro computacional.

El estudio del edificio donde se encuentra ubicado el hardware y los dispositivos que han de soportar nuestras aplicaciones es muy importante, aunque más adelante analizaremos la sala donde se encuentran nuestros sistemas, debemos estar seguros de que el entorno directo de dicha sala (el edificio) cumple con los requisitos de Seguridad Física necesarios.

Aunque lo normal es que las instalaciones estén ya fijadas, es posible que esto no sea así, bien por que la empresa esta cambiando su lugar de operaciones o bien por que es una entidad que esta empezando a operar, nos podemos encontrar con dos posibles situaciones.

a) Partimos de cero

Aun no tenemos un local o edificio para nuestro centro computacional. Aparte del propio inmueble, tendremos que considerar todas las cuestiones del medio externo que lo rodean, de tal forma que la ubicación del inmueble sea la más idónea.

Aquí se realiza el estudio de la localización, que consiste en determinar el lugar adecuado donde sean más favorables los **factores inherentes a la localidad**, vistos anteriormente.

Si nos entramos en está situación debemos, además, comprobar que el local que vamos a destinar para nuestro centro computacional cumpla con la mayoría de requisitos de Seguridad Física referidos al edificio que veremos a continuación o, por lo menos, que sean más fácilmente adaptables para cumplirlos.

b) No partimos de cero

Es cuando en la organización ya se tiene destinado el local o espacio físico y no existe otra alternativa, por lo tanto se debe realizar un estudio de las posibles deficiencias en cuanto a Seguridad Física se refiere y realizar las modificaciones o arreglos necesarios para paliar los posibles riesgos que entrañe.

En este caso, los factores inherentes a la localidad no podrán ser remediados a priori, pero si deben ser estudiados para comprobar el impacto que pueden tener en nuestra entidad y así poder tomar las medidas adecuadas. Si esto fuera muy costoso, se tendría incluso que barajar la opción de un traslado del centro computacional.

En cualquiera de los dos casos, lo normal es que nos encontramos con un entorno ya construido, aunque partamos de cero no es muy común que podamos influir en la construcción del edificio, no modificable y que suele tener un uso compartido por

nuestros sistemas hardware y otro tipo de sistemas. Se intentará siempre resaltar todos los fallos de seguridad que se puedan encontrar, y se tendrá en cuenta si estos son subsanables o inherentes a la estructura del edificio. Se realizará un informe de las posibilidades de modificación para subsanar fallos y de las precauciones que sea posible tomar para minimizar los riesgos de seguridad física cuando no sea posible subsanarlos.

También suele ser interesante estudiar el impacto económico de las modificaciones que consideremos. Nunca se debe dejar de lado ningún defecto que observemos al realizar el estudio, pero las modificaciones que impliquen un gasto considerable deberán ser estudiadas para buscar soluciones alternativas más asequibles que minimicen los riesgos o recurrir, en su caso, a aseguradoras que puedan atenuar la gravedad de un incidente que implique a instalaciones del edificio.

2.3.1 - Suministros de energía eléctrica

El primero de los puntos que debemos observar al realizar el estudio del edificio es el suministro de energía. Como hemos visto anteriormente, es un factor de servicios inherente a la localidad, ya que dependiendo del lugar en el que nos encontremos operará una empresa u otra.

Debemos centrarnos en los suministros de energía que puedan afectar a los **sistemas que queremos proteger**, dejando de lado otras consideraciones como la disponibilidad de servicios para el personal y similares. Por ejemplo es asunto nuestro la disponibilidad de aire acondicionado en la sala de computación, pero no lo es la disponibilidad en la sala de reuniones.

Ahora vamos a ver como evitar las posibles anomalías, como cortes de energía o subidas y bajadas de tensión, que pueden afectar a nuestros sistemas. Hemos de decidir además, qué sistemas requieren este tipo de servicios y cuáles no y el tiempo necesario de corriente desde que se produzca un corte en la red principal.

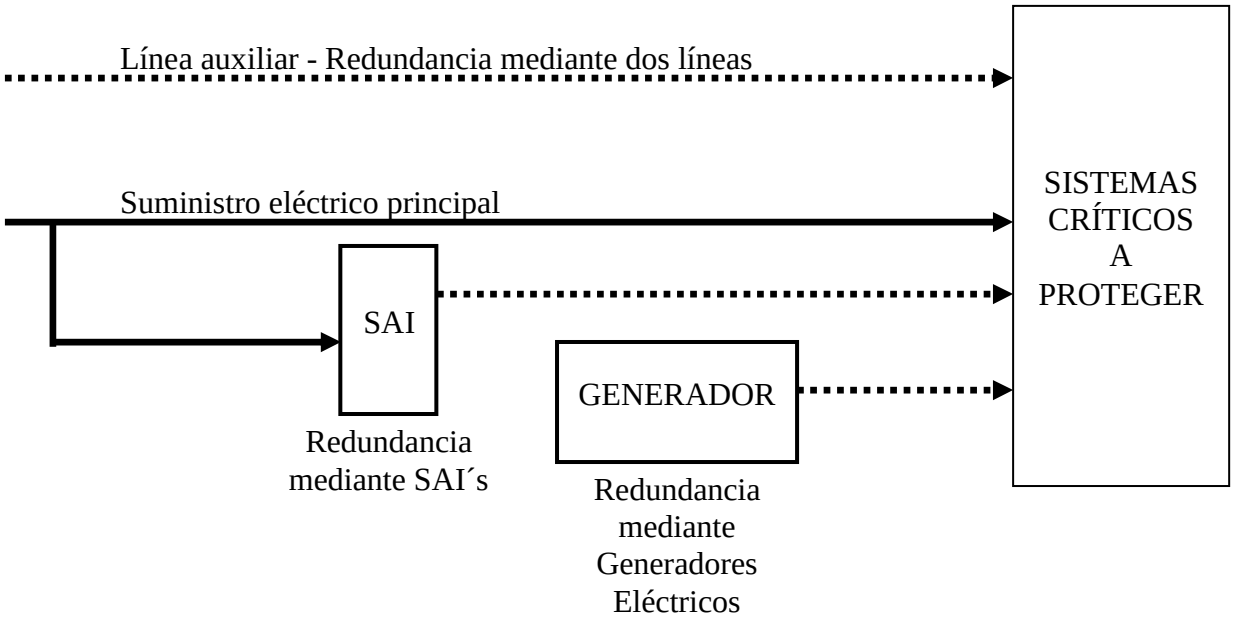
Para evitar los cortes eléctricos en un dispositivo es necesario que exista una **redundancia eléctrica**, es decir, que a nuestros sistemas les llegue la electricidad por, al menos, dos sitios diferentes. De esta manera si la línea principal falla, mediante una línea auxiliar, puedan seguir en funcionamiento. La línea auxiliar de corriente eléctrica solo entra en funcionamiento cuando la principal deja de proveernos de energía eléctrica y como veremos a continuación, puede provenir de **sistemas de alimentación ininterrumpida** (UPS´s o SAI´s), de **generadores eléctricos** o de **otra línea eléctrica independiente** de la principal contratada con un proveedor..

Esquema 2.2

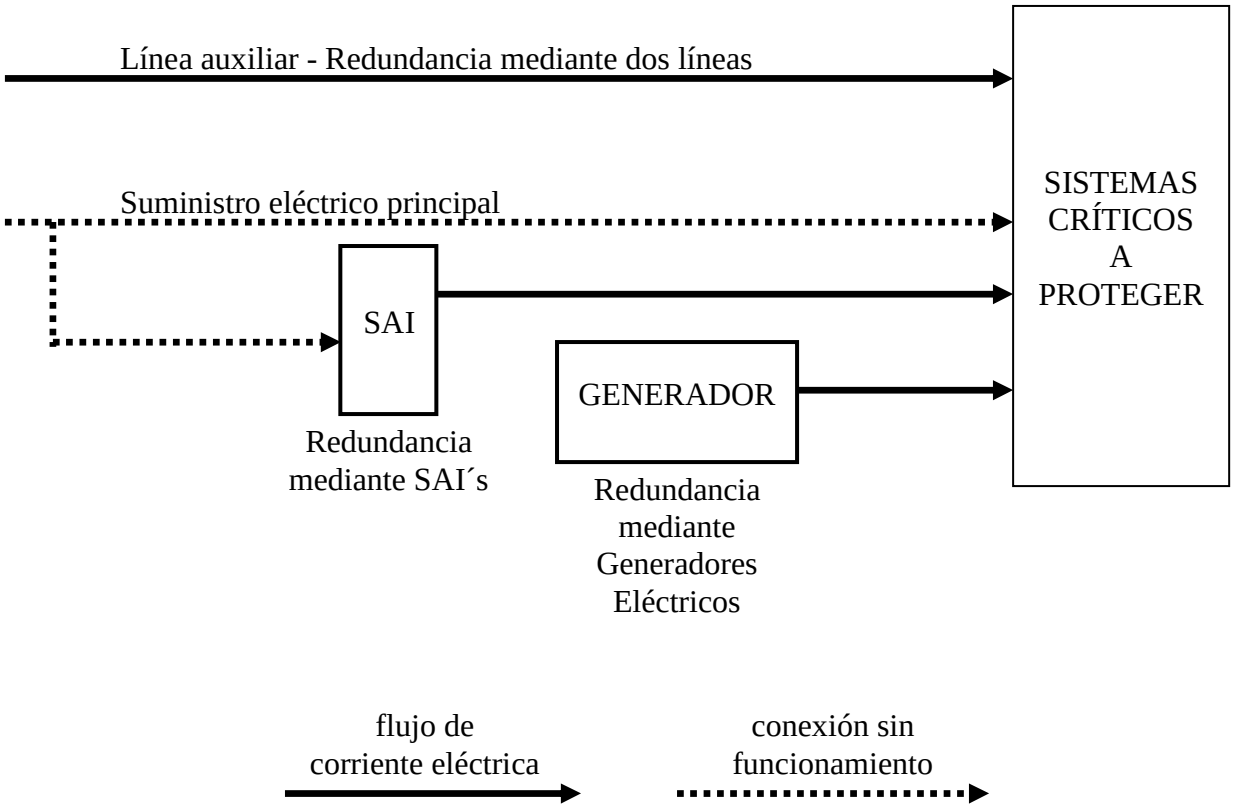
El suministro de energía suele tener dos partes, una parte externa que provee y gestiona la compañía eléctrica y que llega justo hasta el punto donde se encuentra el sistema de tarificación. Detrás del cual se suele encontrar nuestro sistema de protecciones y todo nuestro cableado y dispositivos, la parte interna. Veremos posibles soluciones en ambas partes de nuestra instalación.

Esquema 2.2

a) El suministro llega a través de la Línea Principal



b) El suministro llega a través de alguno de nuestros sistemas de redundancia



a) Parte externa

La parte externa es de la que se encarga la compañía eléctrica, y llega hasta nuestros contadores. Ésta está protegida por un fusible y un limitador que instala la compañía eléctrica y que deben estar calculados para la potencia que vaya a consumir nuestro edificio. Normalmente no deberemos preocuparnos por estos dispositivos, que suelen estar sobredimensionados para evitar cortes de energía y que tienen como principal función la protección de la red eléctrica de la compañía, aunque un punto a comprobar debe ser la posibilidad de que un intruso malintencionado quiera cortar nuestro suministro eléctrico. Para esto debe de comprobarse que no es fácil el acceso a los cables que proporcionan energía eléctrica al edificio, por lo menos en un recorrido razonable desde nuestro edificio hasta la caja de conexiones más cercana.

i) Redundancia mediante dos líneas

Deberemos observar la disponibilidad del suministro de energía a nuestro edificio, teniendo en cuenta la redundancia que pueda tener la red eléctrica y por tanto nuestro suministro eléctrico. Esta información es posible obtenerla llamando al teléfono de información de la compañía eléctrica, que nos informará de la redundancia de la red para nuestro sector en concreto, que suele depender del número de líneas de media o alta tensión de que disponga la compañía en la subestación para proveer de energía al sector donde se encuentre nuestro edificio.

Este es un punto donde no podemos actuar de ninguna forma, simplemente nos podríamos poner al corriente de las posibilidades de la redundancia que estructuralmente se pueda proporcionar al edificio. Este suele ser un aspecto complicado, pues no es común el tener más de una conexión eléctrica para un edificio. Con todo, el sistema ideal sería el que proporcionara redundancia por medio del suministro de energía eléctrica por dos compañías diferentes, claro está, que operen por dos líneas totalmente distintas, ya que si las dos llegan desde el mismo transformador y este falla, fallarán las dos líneas, aunque sean de compañías distintas. Esta es una opción drástica, a considerar solo lo para sistemas críticos. Además, es posible solicitar este tipo de servicios a través de algunas compañías eléctricas y es imposible en otras.

La disponibilidad de este sistema suele ser nula en la mayoría de los sitios, pues aunque se cuente con un mercado de energía liberalizado que permita la contratación del suministro eléctrico eligiendo entre varias compañías, la red eléctrica que ha de transportar esa energía hasta nuestro edificio suele ser propiedad de una de las compañías o de propiedad estatal, con lo que no tendríamos redundancia en el suministro de energía.

b) Parte interna

Como hemos comentado anteriormente, la parte interna de la instalación es la que se encuentra detrás del contador de la compañía e incluye todo nuestro cableado y sistemas de protección y regulación. Es conveniente que personal cualificado, ya sea perteneciente a nuestra entidad o externo a esta, lo revise periódicamente y sea éste el único que lo manipule.

i) Redundancia mediante Sistemas de Alimentación Ininterrumpida

Los sistemas de alimentación ininterrumpida (SAI o en inglés, *UPS Uninterrupted Power Suply*) son unos aparatos, similares a la torre de un PC que se sitúan entre la toma de corriente y el sistema que queremos proteger. Constan de unas baterías en las que van almacenando la electricidad cuando la línea principal esta operativa. Cuando ésta falla, el SAI provee de esa corriente eléctrica almacenada al dispositivo al que esté conectado.

Es la solución más extendida, ya que su instalación es sencilla y su coste es relativamente bajo, los podemos encontrar a partir de 40€. En general, las funciones de estos sistemas son **regular** la cantidad de energía eléctrica que llega al PC, de manera que nos protegen ante posibles subidas o bajadas de tensión y **proporcionar energía** eléctrica de forma continuada, en caso de corte en el suministro de la misma. El tiempo en el que el sistema de alimentación ininterrumpida proporcione energía depende de la capacidad de las baterías y de la carga que tiene que alimentar.

Existen tres tipos de SAI´s, dentro de cada tipo podemos encontrar gran variedad de modelos, cada uno con sus características específicas.

i.i) *Offline o StandBy*
Son los más baratos y su función es dejar pasar tal cual la corriente mientras esta no tenga variaciones de voltaje. Solo cuando esto ocurra entra en acción y suministra corriente desde su batería. Son llamados de NIVEL 3 o gama básica y están recomendados para uso en localizaciones con pocos cortes de red y pocas variaciones de voltaje y adecuados para PC's , cajas registradoras, TPV(10), etc.

(10) (Acrónimo de Terminal Punto de Venta). Se ha venido englobando en esta denominación a varios programas y tecnologías que ayudan en la tarea de un negocio de venta al público. En un mismo aparato se realizan los cobros, cobros con tarjeta, pedidos, consulta WEB, etc.

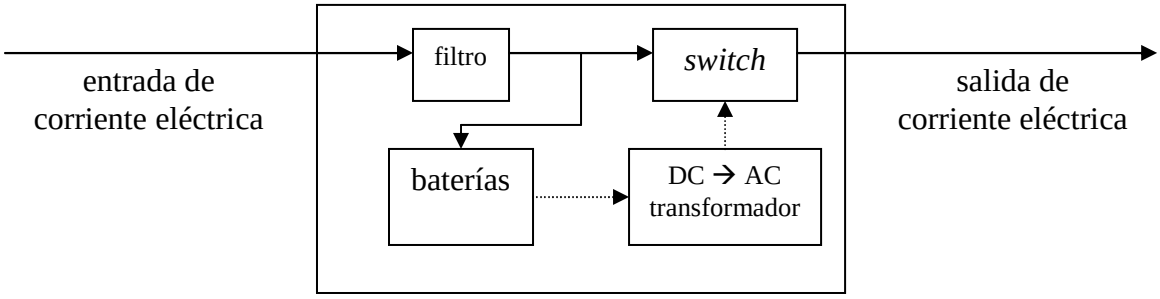
Esquema 2.3

i.ii) *Online o Interactive*
Aparte de la protección del anterior modelo, el SAI filtra toda la corriente que se suministra al PC adaptándola a un estándar. Llamados también de Nivel 5 o Gama Media, al contrario que los de Nivel 3, no producen un micro corte de la corriente al conmutar entre la red y la batería, ya que están actuando constantemente. Son muy fiables y dejan poco lugar a cualquier tipo de problema.

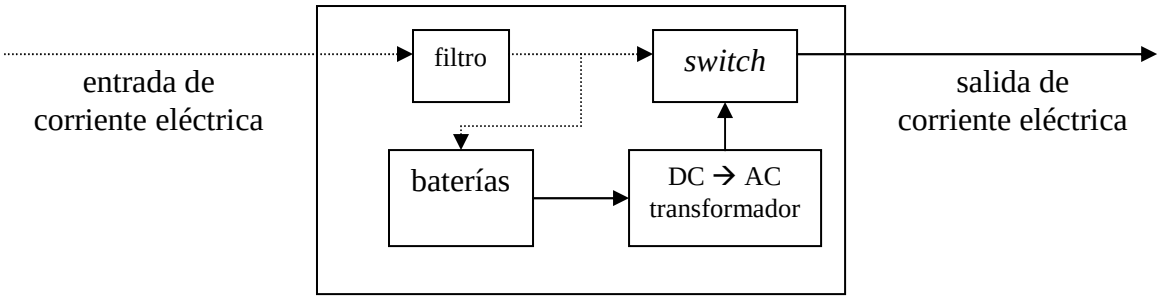
Esquema 2.4

Esquema 2.3

a) SAI *Offline* (nivel 3) con la entrada de corriente operativa

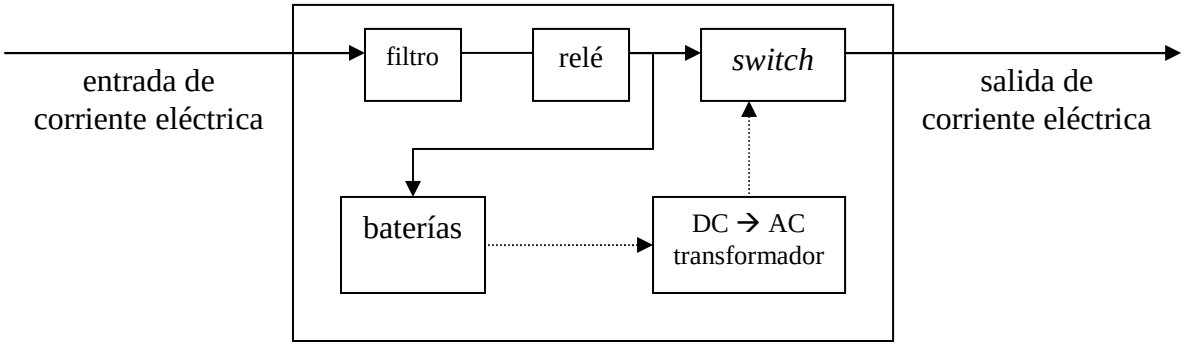


b) SAI *Offline* (nivel 3) sin la entrada de corriente operativa

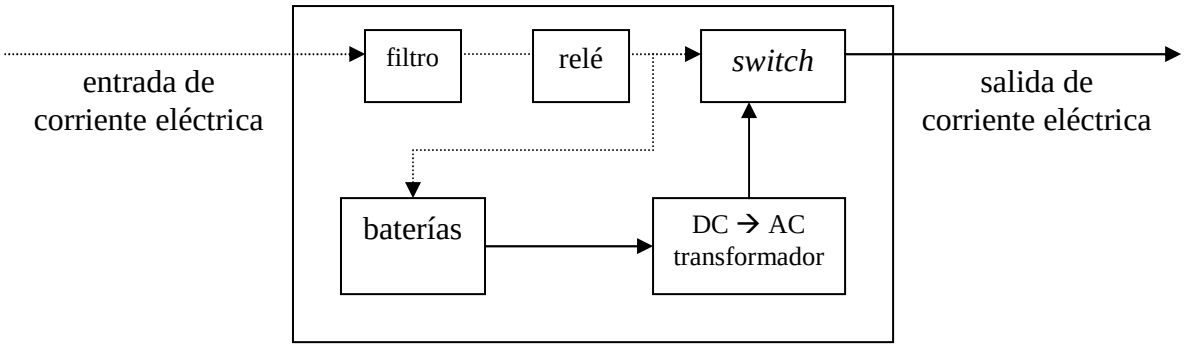


Esquema 2.4

a) SAI *Online* (nivel 5) con la entrada de corriente operativa



b) SAI *Online* (nivel 5) sin la entrada de corriente operativa



i.iii) *Online de doble conversión*
También llamados de Nivel 9, son muy parecidos a los anteriores, sin embargo estos modelos tienen un consumo menor de batería y protegen frente a todos los posibles problemas originados en las líneas de suministro eléctrico. Son para localizaciones donde sean constantes las variaciones de voltaje y haya presencia de ruidos eléctricos.

Esquema 2.5

Como cualquier equipo eléctrico, se deben mantener las condiciones óptimas de que nos indica el proveedor, tales como la temperatura, la ventilación, la humedad, la acústica, etc. Las baterías de los SAI´s son además elementos muy pesados, por lo que el piso debe estar preparado para soportarlo.

ii) Redundancia mediante una planta generadora

La planta generadora de energía es un dispositivo que convierte energía mecánica en energía eléctrica mediante la rotación de bobinas dentro de un campo magnético. Estas se alimentan con un combustible independiente, como puede ser la gasolina, y nos garantizan mucho más tiempo de energía en caso de un corte muy prolongado ya que estos dispositivos pueden funcionar indefinidamente mientras tengan carburante.

En general, los generadores para dar cobertura a todo un área son bastante grandes, a partir de 4 m^3, y pesados, más de una tonelada, aunque podemos encontrar generadores mucho más pequeños y ligeros que pueden dar soporte a dos o tres equipos o un alumbrado de emergencia.

Existe una gran variedad de modelos, por lo que los podemos encontrar de arranque automático o manual, insonorizados o no y pueden ser causantes de vibraciones, calor y/o ruido, factores que habrá que tener en cuenta. Además deben tener una ventilación adecuada, ya que en la combustión se desprende CO_2, así como otras partículas nocivas.

Es posible configurar dos o más generadores independientes para diferentes tipos de cargas, como puede ser el alumbrado de emergencia y los ascensores para desalojar y el centro computacional. Si fuera necesario, se puede recurrir a varios generadores para alimentar la misma carga, todo esto depende de las necesidades de la entidad.

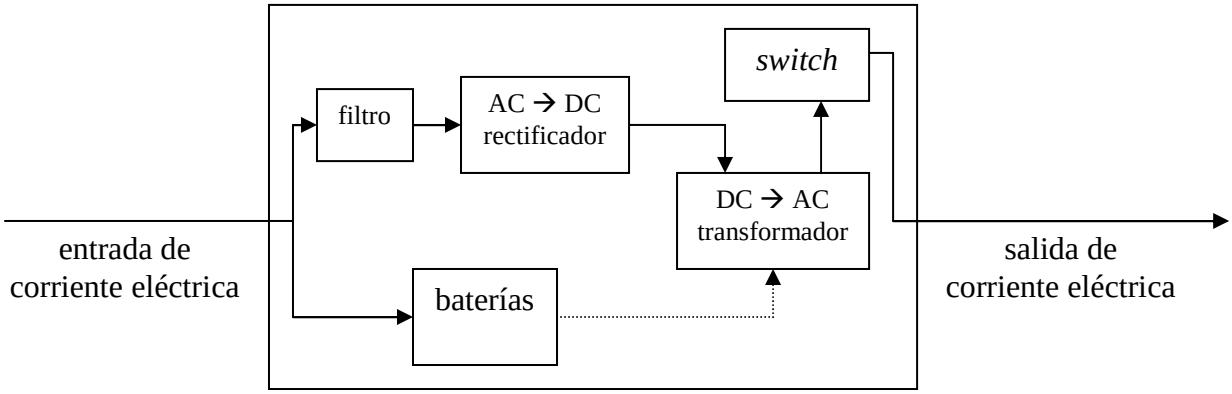
Las plantas generadoras de energía se pueden clasificar en base al combustible que utilizan. Solo contemplamos los dos tipos habituales empleados como grupos auxiliares, **diesel** y **gasolina**, ya que una planta generadora puede ser desde un molino de viento hasta una central nuclear.

A efectos del usuario, tanto los generadores diesel como los generadores gasolina son muy similares, la potencia de salida varía desde los 2kV hasta los 100kV. Indicar que 1kV equivale a 1.000V y que un ordenador personal consume del orden de 200V a 400V.

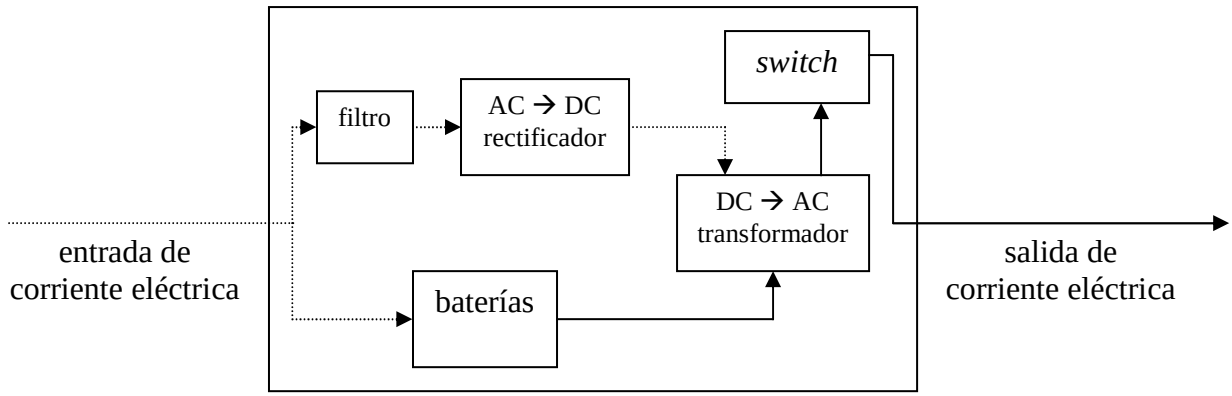
Aparte del generador en si, habrá que tener presente la necesidad de almacenar el combustible de éste, por lo que se tomarán las medidas de seguridad necesarias al respecto.

Esquema 2.5

a) SAI *Online de doble conversión* (nivel 9) con la entrada de corriente operativa



b) SAI *Online de doble conversión* (nivel 9) sin la entrada de corriente operativa



2.3.2 - Los enlaces de comunicaciones del edificio

El caso de los sistemas de comunicaciones del edificio es similar al del suministro eléctrico, deberemos buscar la mayor seguridad y protección en los sistemas y además siempre que sea posible tener redundancia en los sistemas de comunicaciones para prever el caso de que uno de los enlaces falle. Los sistemas de comunicaciones suelen ser de dos tipos, **públicos** y **privados**.

a) Sistemas de comunicación públicos

La mayoría de los edificios usarán estos sistemas de comunicaciones y será la que nos de salida al exterior. Esta puede ser la red telefónica para el transporte de voz y datos o las conexiones ADSL(11), DSL(12), Cable, etc. que usan medios compartidos para la transmisión de datos.

(11) (de *Asymmetric Digital Subscriber Line* "Línea de Abonado Digital Asimétrica"). Consiste en una línea digital de alta velocidad, apoyada en el par trenzado de cobre que lleva la línea telefónica convencional. La velocidad de envío y recepción de datos es distinta.

(12) (de *Digital Subscriber Line* "Línea de abonado digital") Es un término utilizado para referirse de forma global a todas las tecnologías que proveen una conexión digital sobre línea de abonado de la red telefónica local. La velocidad de envío y recepción de datos es la misma.

Para los sistemas públicos debemos estudiar sobre todo si existe algún tipo de redundancia en las comunicaciones, puesto que las compañías telefónicas que suelen ser las que proveen los servicios no suelen proporcionar ningún tipo de certeza de que nuestras comunicaciones van a mantenerse, por lo que estamos a expensas de las averías o fallos que se puedan producir en las redes públicas para tener comunicaciones.

Es un sistema bastante común en grandes edificios y no debería tener más complicaciones. Es muy normal que las compañías que usan la red telefónica clásica compartan el medio físico para mandar los datos, medio físico que será propiedad pública o de una de las compañías, pero en cambio las compañías de cable suelen tener su propia red para proporcionar la conectividad, por lo que puede ser interesante la contratación de una línea con una compañía tradicional y otra con una compañía de cable para tener dos redes independientes.

En el caso de que dispongamos de dos o más líneas de comunicaciones es necesario que el departamento de administración de red lo tenga en cuenta para poder dirigir el tráfico de forma que si uno de los enlaces falla los datos se transmitan por otro enlace. Esta estructura de acceso a redes es muy común en grandes instalaciones y no debería haber problema en su implantación.

b) Sistemas de comunicación privados

Los sistemas de comunicaciones privados son los que nos permiten comunicar nuestros edificios o servidores mediante un cable directo. Puede que simplemente unan varios PC´s en una sala, varias impresoras o servidores o que conecte, incluso, varios edificios de nuestra propiedad. Así podemos hacer que todos nuestros equipos estén conectados a uno central que de salida exterior, pudiendo aplicar filtros y medidas de seguridad especiales solo a este equipo central.

Para los sistemas privados las consideraciones de seguridad son algo menos severas que para los sistemas compartidos, ya que la compañía que nos suministra el servicio nos asegurará las conexiones con una tasa fija de porcentaje de fallo en el tiempo, lo que nos permite planificar más fácilmente la seguridad del enlace, pues tenemos la seguridad de que este se mantendrá. Lo mismo se aplica para los sistemas de comunicaciones privadas entre edificios usando microondas, donde se colocan emisores y receptores de ondas y se emplea el aire como canal de datos. Nosotros mismos podemos asegurar la comunicación y no dependemos de la disponibilidad de una red pública.

Para estos sistemas privados se puede realizar un estudio contratando a personal especializado en estos enlaces y en su ajuste. Siempre es aconsejable complementar estos sistemas privados con un sistema de comunicación público para proporcionar redundancia en el caso de que nuestro enlace falle.

Se comprobará también la seguridad física del cableado (o la visibilidad de los tambores de microondas en su caso) comprobando que un intruso malintencionado no pueda seccionar los cables de comunicaciones que van desde la centralita más cercana hasta nuestro edificio. Hay que tener en cuenta que esta sección de cable es propiedad de la compañía que proporciona el servicio, por lo que necesitaremos llegar a un acuerdo con esta si queremos realizar algún tipo de modificación en este cable.

Esquema 2.6

2.3.3 - Otros suministros del edificio

Aunque menos importantes, existen otros suministros precisos para el buen funcionamiento de nuestra entidad, como son **el agua**, **el gas** y **el gasoil**. Vamos a ver como pueden influir sobre la Seguridad Física de nuestros sistemas.

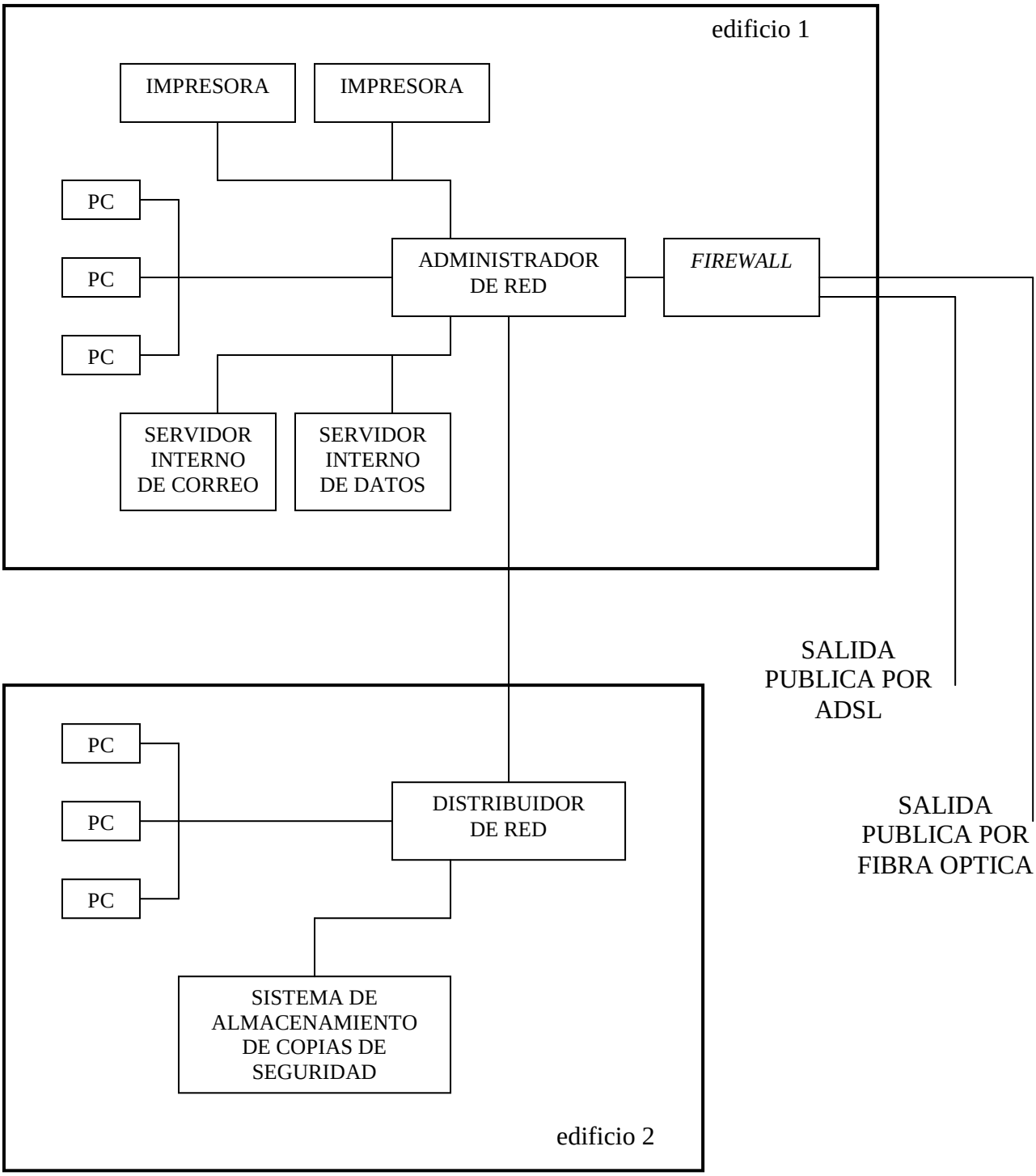
a) El gas y el gasoil

Deben tenerse en cuenta su suministro ya que algunos sistemas de calefacción funcionan con gas o gasoil y pueden ser necesarios en climas muy fríos para mantener una temperatura mínima en nuestros centros de datos. Aunque sólo afectaría a nuestros sistemas si la temperatura fuera extremadamente baja, ya que el frío no suele ser un problema para los sistemas hardware, si no un factor favorable.

El suministro de gas nos puede llegar de distintas maneras, por tuberías o por depósitos. El de gasoil suele llegar exclusivamente por depósitos.

Esquema 2.6

Enlaces de comunicaciones del edificio, sistema completo



i) Por tuberías
Si el suministro de gas nos llega a través de tuberías debemos velar por que no se pueda acceder a éstas con facilidad y sean manipuladas exclusivamente por personal cualificado.

ii) Por depósitos
Si no disponemos de un servicio directo de gas por tuberías, lo cual es normal fuera de las grandes ciudades, o nuestro sistema de calefacción funciona con gasoil, lo normal es que dispongamos de un depósito para su almacenaje. Éste lo suelen proveer las compañías que nos ofrecen el servicio de suministro y dado que guardan un combustible altamente inflamable, su acceso debe ser restringido y solo lo manipulará el personal cualificado. Además se tomarán las medidas antiincendios oportunas, de las cuales hablaremos más adelante.

b) El agua

El agua suele llegar a nuestro edificio por una única tubería y es competencia de la administración pública su abastecimiento. Al igual que el gas o el gasoil, puede que nuestros sistemas de calefacción necesiten de agua para funcionar.

Sin embargo, como más nos puede afectar la falta de suministro de agua es si es necesaria para el correcto funcionamiento de nuestros sistemas de extinción de incendios. Por lo tanto, se deberán tomar las medidas oportunas para que si se produjera un corte en el abastecimiento de agua, dichos sistemas de extinción pudieran seguir operativos.

2.3.4 - Los accesos físicos al edificio

Siguiendo la estructura del proyecto, vamos a ver ahora los accesos físicos al edificio. Entendemos que el edificio entero será propiedad de la entidad, si por el contrario la entidad cuenta con solo unas oficinas o incluso un solo despacho, el tema que tratamos en este punto se reduce al acceso físico de dichas oficinas o despacho. Más adelante veremos el acceso físico a espacios más críticos, como la sala donde se encuentran los servidores o el centro computacional.

Debemos tener en cuenta que el edificio tiene una serie de accesos obvios y otros no tan obvios que un intruso puede usar para entrar en nuestras instalaciones. Los obvios son las puertas principales de acceso y las ventanas que se encuentran cercanas a la calle. Los no tan obvios son las puertas de servicio, las ventanas superiores, las claraboyas, los accesos de mantenimiento o los sistemas de ventilación o calefacción, por lo que podemos hablar de **entradas en servicio** y **entradas ocultas**.

a) Entradas en servicio

Son las entradas que se usan normalmente, tanto por el personal de la entidad como por los usuarios, los empleados de mantenimiento o los posibles clientes. En estos accesos lo que se debe de tener es un control de quién y cuándo puede acceder. Podemos hablar

ahora de las normas **UNE-EN 50133 Sistemas de control de accesos para uso en aplicaciones de seguridad** y la **UNE-EN 50136 Sistemas y equipos de transmisión de alarma**.

El disponer de un sistema de validación nos puede suponer otras ventajas, como es que a la vez que se valida el personal quede reflejada la hora para controlar el tiempo de trabajo diario o conocer la gente que está dentro de las instalaciones ante una emergencia, como un incendio. Con la tecnología de hoy en día esto no supone un gran esfuerzo económico para una entidad.

La validación en la entrada del edificio debe ser más rigurosa si una vez que hemos accedido a éste podemos entrar en cualquier zona, incluyendo las más críticas. Por el contrario, si aunque estemos dentro del edificio no podemos acceder a ninguna zona sensible, la validación al entrar en el edificio podrá ser más relajada.

Los sistemas de validación deben ajustarse a nuestras necesidades pero también a las de las personas que lo vayan a utilizar, es decir, para acceder al edificio, lo normal será que el proceso de validación sea casi instantáneo, no podemos pretender que todo el personal de una entidad pase por varios sistemas de validación y emplee diez minutos cada mañana al incorporarse al trabajo.

Estos sistemas se pueden dividir en tres grupos: por **algo que se sabe**, por **algo que se es** y por **algo que se posee**.

i) Algo que se sabe
Es lo más normal para acceder a los terminales, y el ejemplo más claro es el de introducir la contraseña al iniciar la sesión en un ordenador (se sabe la contraseña). No es muy normal para acceder a los edificios, pero lo veremos más adelante.

ii) Algo que se es
Factores inherentes del individuo y que podemos analizar biométricamente. Los más empleados son los análisis de retina, de voz, de huella digital o de la palma de la mano. Estos sistemas no suelen emplearse en las entradas principales de los edificios, aunque si para acceder a salas más críticas o incluso a equipos en concreto. Los veremos más en profundidad más adelante.

iii) Algo que se posee
Como una llave o una tarjeta. Es el más utilizado para los accesos generales a los edificios ya que normalmente el personal de la entidad cuenta con una tarjeta para validarse y a la vez fichar la hora de entrada y salida. Por ser un sistema cómodo para los usuarios, también se emplea para acceder a salas o despachos, zonas sensibles y últimamente se está imponiendo como sistema para validarse en los PC´s sustituyendo al tradicional sistema de usuario y contraseña.

Normalmente las puertas principales de los edificios están abiertas y el sistema de validación por tarjeta se emplea en el interior, ya sea simplemente fichando en un reloj o mediante un sistema de tornos que restrinjan el acceso. Al no ser que empleemos un sistema que impida físicamente el paso deberemos tener un vigilante de seguridad o un

recepcionista que verifique que todo el que accede al edificio lo hace de la manera correcta.

Si la entidad es pequeña o disponemos de unos despachos dentro de un edificio, lo normal es que utilicemos un sistema tradicional de cerradura de seguridad y empleemos una llave para acceder.

b) Entradas ocultas

Entendemos por entradas ocultas todos aquellos lugares por los que, aún no siendo entradas, se podría acceder al edificio, como por ejemplo conductos de ventilación, ventanas, desagües o incluso, paredes débiles que faciliten un butrón o falsos techos, por lo que si fuera necesario, debemos hacer un estudio de los planos arquitectónicos del edificio.

En este tipo de entradas y donde sea posible, lo que se debe hacer bloquear el paso de alguna manera, ya sea mediante rejas, blindajes, etc. Allí donde no sea posible bloquear el paso se deben colocar detectores de intrusos, ya que sea quién sea el que acceda por una entrada oculta lo hará por un sitio no permitido y si no podemos impedir su paso, por lo menos debemos tener conocimiento de que ha accedido alguien.

Claro está que no podemos colocar rejas o barreras sin tener conocimiento de lo que estamos haciendo, ya que podríamos bloquear desagües, conductos de ventilación, salidas de emergencia, etc. Además hay que tener en cuenta que existen ciertas zonas donde puede que en un momento dado se tenga que acceder, a como una cañería principal en el sótano o un conducto eléctrico en el subsuelo para, por ejemplo, realizar una reparación.

Como todas las medidas de Seguridad Física, hay que hacer hincapié en que este aspecto debe ser proporcional a lo críticos que sean los datos que queremos salvaguardar, ya que no es lo mismo la oficina de una pequeña empresa, donde puede haber datos de sus clientes o proveedores que la oficina central de un banco.

Podemos realizar una distinción entre la vigilancia en **horas de oficina** y cuando el **edificio está cerrado**. En horas de oficina nuestra atención se centrará en el control de accesos y las entradas ocultas contarán con una seguridad pasiva, es decir, accesos bloqueados o sensores de movimiento. Durante las horas que el edificio esté cerrado todas las entradas contarán con este tipo de seguridad, ya que estarán bloqueadas o contaran con algún sistema que detecte una posible intrusión. Algunos de estos sistemas de detección tienen también un factor disuasorio, por lo que podrían ser además sistemas de prevención. Veremos los más comunes a continuación.

2.3.5 - Sistemas para detectar intrusiones

Independientemente de la tecnología que empleen, los sistemas para detectar intrusiones constan de tres partes fundamentales: la **unidad de control,** uno o más **sensores** y uno o más **anunciadores**. Cuando un sensor detecta algo, envía una señal eléctrica al panel de

control y éste, si está activado, transmite la indicación oportuna a los anunciadores para que se pongan en funcionamiento. Existe una norma, la **UNE-EN 50131 Sistemas de alarma de intrusión**, que nos establece unos estándares al respecto.

Es importante saber que todos estos sistemas forman parte de los sistemas que deben estar siempre operativos, por lo que deberán tener algún sistema de redundancia eléctrica de los vistos anteriormente, para que si se produjera un corte en el suministro principal, pudieran seguir operativos. Algunos dispositivos o sistemas al completo cuentan con sistemas de baterías que les otorgan una cierta autonomía, en cualquier caso, se tendrá que controlar este aspecto.

a) La unidad de control

También llamada caja de control o panel de control es el cerebro del sistema. Podemos tener muchos sensores, incluso de tipos muy dispares, pero no es necesario por ello tener varios paneles de control ni varios anunciadores, todos los sensores al ser activados envían una señal al panel de control y este, si está programado para ello, envía la señal a los anunciadores, que serán los mismos, independientemente del sensor que detecte la intrusión. Podemos programar nuestro sistema para que dependiendo de qué sensor detecte una intrusión o de cualquier otro factor, como el momento del día que nos encontremos, haga una cosa u otra.

El interfaz [(13)] entre el sistema y el usuario es lo que se llama **teclado** y es el medio para programar, activar y desactivar. Normalmente existe un único panel de control pero podemos tener varios teclados para activar o desactivar nuestro sistema, por ejemplo, en distintas puertas. Incluso, para mayor comodidad, existen teclados a control remoto que permiten operar a una cierta distancia de la unidad de control o del receptor del dispositivo y se están implantando sistemas que se pueden operar desde un teléfono móvil o conectándose a Internet.

[(13)] Instrumento que permite la interrelación entre el usuario y otro dispositivo, en este caso, el sistema de alarma.

b) El anunciador

Es lo que realiza el efecto de nuestro sistema cuando, estando activado, detecta una intrusión, y por tanto, permite saber que la alarma ha sido activada. Básicamente podemos encontrar dos tipos de anunciadores, **sonoros** y **silenciosos**, aunque ambos tipos se complementan.

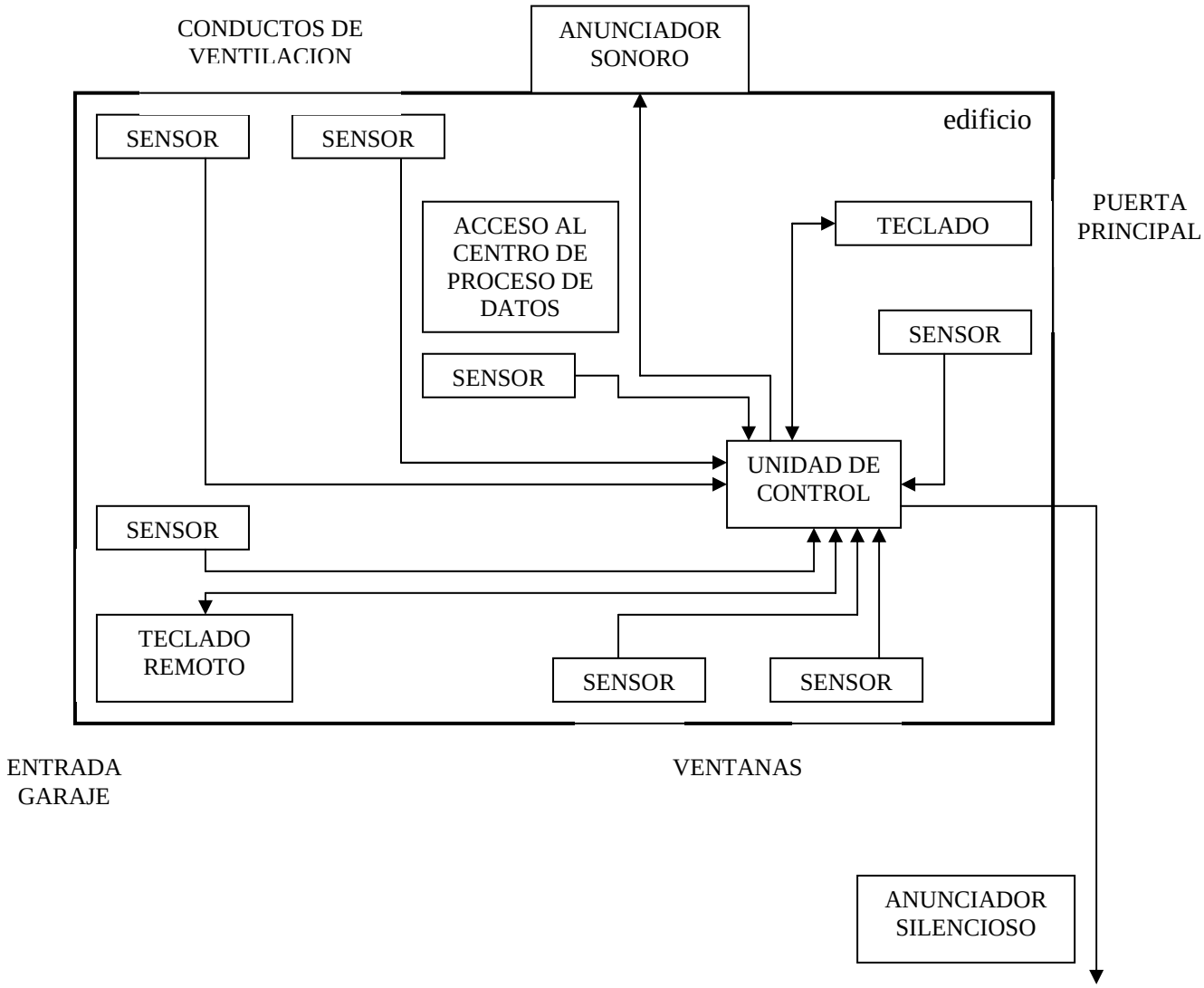
i) Anunciadores sonoros
Son los anunciadores tradicionales, los que generan una alarma luminosa y/o acústica. Normalmente estos anunciadores emiten ambas al tiempo y dependiendo de cómo hayamos programado nuestro sistema, se detienen pasados unos minutos. Como suelen estar colocados a la vista, estos anunciadores tienen un efecto disuasorio.

ii) Anunciadores silenciosos

Tradicionalmente los anunciadores silenciosos emitían una señal a nuestra compañía de seguridad o a las fuerzas de seguridad del estado, indicando que en nuestra entidad se está produciendo una intrusión. Aunque esto se sigue manteniendo y es fundamental, para complementar este aviso, hoy en día podemos encontrar anunciadores que realicen cualquier acción para la que haya sido programados, como bloquear puertas, cortar la corriente eléctrica, aislar zonas concretas o, incluso, enviar avisos a teléfonos móviles.

Esquema 2.7

Sistema de detección de intrusiones



c) Los sensores

Los sensores o detectores vienen en una gran variedad de formas y tamaños, y están diseñados para detectar sonidos, movimiento del aire, calor corporal y otras condiciones que indican la presencia de un intruso, así como rotura de cristales, apertura de puertas, etc.

Los sistemas más comunes que podemos emplear para detectar intrusiones son **detectores espaciales**, **barreras infrarrojas**, **detectores de rotura de vidrio**, **detectores perimetrales**, **detectores por presión** y **cámaras de vigilancia**. Como veremos más adelante, estos sistemas no solo se pueden emplear para controlar las entradas del edificio, si no también para vigilar todo lo que sucede en el interior de éste. Podemos decir también que estos sistemas se complementan entre sí y es necesario conocer las deficiencias de uno para suplirlas con otro.

Hoy en día podemos encontrar sensores de reducido tamaño, empotrados o incluso personalizados para que no desentonen con nuestro mobiliario. Aparte de la posible mejora estética, su fin es que los posibles intrusos no se percaten de la presencia de éstos. Sin embargo es recomendable que al menos uno de nuestros sistemas esté a la vista para que de ésta manera tenga un efecto disuasorio.

i) Detectores espaciales

Los detectores espaciales captan cualquier movimiento o cambio de parámetros en su campo de acción. Son una parte muy importante en los sistemas de detección de intrusos, especialmente en los casos en lo que la entrada no ha sido forzada. Existen varios tipos.

i.i) Detectores por infrarrojos

También llamados sensores PIR, son el tipo de sensor más común y podemos diferenciarlos en dos tipos, sensores PIR **activos** y **pasivos**. Los pasivos los vamos a ver en este punto, dado que los clasificamos dentro de detectores espaciales. Los activos los veremos más adelante, ya que pertenecen al grupo de barreras infrarrojas.

Los **sensores PIR pasivos** son sensibles a las ondas de luz infrarroja, las cuales son invisibles al ojo humano. La energía infrarroja se puede detectar en forma de calor, y este tipo de sensores detectan el calor irradiado por una persona u otro cuerpo. Los circuitos electrónicos permiten que el detector reconozca la cantidad normal de calor habitualmente presente en el área. Al ingresar un intruso, el calor irradiado por su cuerpo se suma a la cantidad de calor normalmente presente en el área, el sistema detecta un aumento de la energía infrarroja y envía un señal a una alarma.

Los sensores PIR son muy sensibles a los cambios de temperatura, pero no pueden “ver” a través de objetos macizos y tampoco a través del vidrio, por lo que son más fáciles de configurar que los detectores por ultrasonido o por microondas. Hay que tener en cuenta que sí deben obviar los cambios graduales de temperatura, como los producidos por la luz solar o la calefacción.

Otra cualidad de estos sensores es que no ven la totalidad del espacio controlado, si no que tienen patrones de detección específicos y limitados, que son determinados por su lente. Una manera de visualizar un patrón de detección es imaginar cinco o más largos "dedos" invisibles que salen del sensor PIR en diferentes direcciones y que activan la alarma cuando alguien toca uno de los dedos. Por lo que los espacios entre los dedos no son cubiertos por el sensor PIR.

Teóricamente éste problema se podría solucionar instalando múltiples sensores PIR, pero aún así no se podría cubrir todos y cada uno de los puntos del campo vigilado. Sin embargo rara vez se necesita más de uno de estos. La solución al problema mencionado consiste en elegir el tipo de lente correcto que permita lograr la cobertura correcta para el área que se desea proteger. Dado que el sensor PIR no emite nada, para un posible intruso será imposible saber por donde pasan cada uno de esos "dedos".

Existen también los **sensores PIR cuádruples**, que consisten en dos sensores de elemento dual en un solo chasis. Cada sensor tiene circuitos procesadores independientes, es decir que el detector es básicamente dos sensores en uno. Los sensores cuádruples reducen las falsas alarmas porque ambos sensores PIR deben detectar la presencia de un intruso antes de activar la alarma.

i.ii) Detectores por ultrasonido

Algunos sistemas de alarma antirrobo de diseño más antiguo utilizan ultrasonido (sonido de muy alta frecuencia) para detectar movimiento. En estos detectores un transmisor envía un sonido de una frecuencia tan alta que no es perceptible para el oído humano. Un receptor recoge las ondas sonoras reflejadas por la habitación o área protegida. Si alguien o algo se mueve en el espacio comprendido entre el receptor y el transmisor se producirá un cambio o modificación de la frecuencia del sonido, entonces, un circuito del dispositivo que detecta cualquier cambio inusual de la frecuencia activará la señal de alarma.

Los detectores ultrasónicos son extremadamente sensibles, y algunas veces pueden ser activados por ruidos, como un teléfono al sonar o las llaves moviéndose en un llavero, o corrientes de aire, por lo que deben ser configurados para que estos sonidos o los cambios pequeños, como los que podrían producir un insecto o roedor, sean ignorados.

Los cambios de frecuencia descriptos en el párrafo anterior también se conocen como efecto *Doppler*. Este efecto es el resultado del comportamiento de las ondas sonoras cuando son comprimidas por un objeto en movimiento.

i.iii) Detectores por microondas

Al igual que el anterior, es un dispositivo de protección espacial muy sensible. Los detectores de microondas emiten ondas de radio de alta frecuencia y detectan cualquier cambio en el patrón de las ondas reflejadas que pudiera provocar un intruso.

Los detectores de movimiento de microondas también utilizan el efecto *Doppler*, pero en lugar de emitir un sonido, estos detectores emiten energía electromagnética en forma de microondas. Una característica de la energía de microondas es que penetra el vidrio, muros y otros cuerpos. Por esto, los detectores de microondas son fáciles de ocultar ya que se pueden colocar detrás de otros objetos, pero son difíciles de regular correctamente. Un automóvil que pasa, las transmisiones de radio e incluso las luces fluorescentes pueden activar una falsa alarma.

i.iv) Detectores combinados

En principio se podrían combinar cualquier tipo de sensores (hemos visto ya los sensores PIR cuádruples, que combinan dos sensores PIR), pero lo más normal es combinar un sensor PIR con un detector de microondas, ya que los parámetros que miden son distintos. Con ello se obtienen los **dispositivos de tecnología dual**.

Estos dispositivos sólo activan una alarma cuando ambos tipos de sensores detectan una violación. Un movimiento que se produce por una corriente de aire podría activar el sistema de microondas pero no afectará un sistema de tecnología dual porque el sensor PIR no notaría simultáneamente un cambio de la radiación infrarroja. Los dispositivos de tecnología dual pueden ser más costosos y difíciles de configurar correctamente, pero son mucho más fiables y evitan un gran número de falsas alarmas.

ii) Barreras infrarrojas

Cada barrera se compone de dos partes, un emisor que envía continuamente uno o más haces infrarrojos invisibles en forma pulsada y codificada y un receptor que capta dichas señales. Cuando algo o alguien se sitúa entre el emisor y el receptor atravesando ese haz, se interrumpen la recepción y la detección es informada a la central de control.

Existen modelos tanto para interior como para exterior y pueden tener un alcance entre emisor y receptor de más de 100 metros. Habrá que tener muy en cuenta las características del modelo que instalemos, ya que factores como los cambios de temperatura o de luz pueden alterar a su funcionamiento, pudiendo producir falsas alarmas.

Estos dispositivos pueden contar con protección *antidesarme*, esto es, que si alguien intenta abrir la tapa para desarmarlo envían una señal a la central de control para que salte la alarma. El haz de luz infrarroja puede ser doble o cuádruple, para dar mayor fiabilidad al sistema. Además podemos especificar el tiempo que debe estar cortado el haz para que se active, evitando de esta manera falsas alarmas.

iii) Detectores de rotura de vidrios

Éstos detectores se basan en la característica señal multifrecuencia que produce el quiebre de un vidrio. No importa si el vidrio es laminados, vidrios placa, templados o alambrados, ya que el sistema detecta la rotura de cualquier tipo de vidrio. Además los

microprocesadores incorporados en estos dispositivos le permiten discriminar e ignorar sonidos que pueden causar falsas alarmas.

Los detectores de rotura de vidrios deben ser ubicados en cualquier lugar cerca de puertas y ventanas de vidrio o con vidrio, en estantes, camuflados detrás de otros objetos o empotrados en paredes o suelos. Aunque depende de las características del dispositivo en concreto, normalmente tienen un alcance de unos 10 metros, por lo que protegen varias ventanas y puertas simultáneamente. Existen también detectores *omnidireccionales* que se pueden colocar el techo dando una mayor cobertura.

Algunos modelos con tecnología dual incorporan sensores que detectan vibraciones. Éstos se colocan en cada una de las puertas y ventanas de tal manera que para que se active la alarma no solo tiene que detectarse el sonido de la rotura del vidrio, si no también la vibración que se produce. De esta manera se reducen las falsas alarmas.

iv) Detectores Perimetrales

Los sensores perimetrales son colocados en puertas y ventanas y envían una señal cuando éstas se abren. El más popular es el interruptor magnético ya que son confiables, económicos y fáciles de instalar. Consiste de dos componentes, un interruptor y un imán, generalmente ambos albergados en un chasis de plástico de forma idéntica. El interruptor contiene dos contactos eléctricos y una barra metálica con resorte que puentea el contacto mientras se aplica magnetismo, permitiendo que el circuito eléctrico del sistema de alarma esté completo (no interrumpido). Cuando la fuerza magnética no está presente, la barra levanta uno o ambos contactos, creando un circuito abierto y activando la alarma. De este modo funcionan los interruptores magnéticos de la mayoría de los sistemas de alarma antirrobo.

En una instalación típica, el imán se instala en una puerta o ventana y el interruptor se instala en el marco, alineado con el imán a una distancia de aproximadamente uno o dos cm. Cuando un intruso empuja la puerta o ventana para abrirla, el imán sale de alineación y ya no mantiene la barra del interruptor sobre los contactos. Algunos interruptores magnéticos están diseñados de manera tal que pueden ser instalados en superficie.

Para lograr una instalación más atractiva, algunos prefieren interruptores magnéticos empotrados. Los modelos para empotrar se instalan en orificios perforados. Si están correctamente instalados, los interruptores magnéticos empotrados son difíciles de detectar y se disimulan muy bien en la puerta o ventana.

v) Detectores por presión

Los detectores por presión están colocados en el suelo y tienen el aspecto de una alfombra o felpudo de goma. Cuando una persona los pisa, la presión ejercida sobre éstos es detectada por los sensores y envían la señal de alarma a la unidad de control. Son ideales para colocarlos tras las puertas de acceso al edificio y en sitios por los que el paso para acceder a éste sea obligado.

Aunque son sistemas baratos, su instalación es algo más aparatosa que la de otros sistemas de detección de intrusiones y además su escasa duración y fácil vulnerabilidad hace que sea un recurso poco empleado.

vi) Cámaras de vigilancia

Las cámaras de vigilancia son artefactos que recogen imágenes para su posterior tratamiento, visionado o almacenaje. Aunque a efectos prácticos son muy parecidas, debemos diferenciar dos grandes grupos, **sistemas digitales** y **sistemas analógicos**.

Ambos nos ofrecen la posibilidad de ver que es lo que está ocurriendo en un área concreta en tiempo real, por lo que es mucho más completo que cualquier otro método de detección. Sin embargo es necesario que las imágenes obtenidas por las cámaras de vigilancia sean monitorizadas constantemente, ya sea por humanos o por *software*.

Además estos sistemas nos permiten grabar las imágenes obtenidas para posibles investigaciones posteriores. Es muy recomendable el realizar éstas grabaciones y guardarlas, al menos, una semana. En la imagen obtenida es también muy recomendable que aparezca el momento y el lugar de la grabación, es decir, fecha, hora y qué cámara (si es que tenemos más de una) realizó la grabación.

Si disponemos de más de una cámara, no es necesario disponer de un monitor por cada una de éstas, ya que estos sistemas permiten rotar la imagen visionada en intervalos cortos o ver simultáneamente la imagen de más de una cámara en el mismo monitor.

vi.i) Sistemas analógicos

Son los sistemas tradicionales. La imagen es captada por una cámara y ésta envía la señal de vídeo hasta un monitor para que sea visionada por un vigilante y hasta un aparato grabador para que sea almacenada en un medio magnético. Existen grabadores de velocidad superlenta que permiten almacenar en una cinta convencional VHS hasta 24 horas ininterrumpidas perdiendo muy poca calidad de imagen.

En estos sistemas el vigilante debe estar constantemente viendo las imágenes para percatarse ante cualquier intrusión o anomalía. Una ventaja del sistema de vigilancia por cámaras es que si un intruso entra en nuestras instalaciones y pasa por delante de una cámara pero el vigilante no se percata de ello, éste podrá ver cualquier rastro que deje a su paso, como huellas, cristales rotos o puertas abiertas.

vi.ii) Sistemas digitales

Los sistemas digitales son más modernos y ofrecen un mayor número de posibilidades, sobre todo para automatizar la labor de vigilancia, sin embargo es difícil que alcance la calidad de imagen que ofrecen los sistemas analógicos.

En este tipo de sistemas la imagen que es recogida por la cámara es enviada a un elemento *hardware* donde es procesada. La imagen se puede mostrar en un monitor para

que sea visionada por un vigilante pero también puede ser analizada por un programa que, mediante los cambios entre fotogramas, detecte movimiento y haga saltar la alarma, por lo que estos sistemas no precisan de un vigilante. Además pueden incorporar un disco duro en el propio *hardware* para almacenar las imágenes recibidas.

Normalmente estos elementos incorporan un conversor a analógico para que la imagen salga por una clavija convencional y pueda ser almacenada en un medio externo o visionada en un monitor tradicional.

Al margen de esto, podemos encontrar cámaras **inalámbricas** que emiten la señal de vídeo por radiofrecuencia, sin necesidad de cables, lo que facilita muchísimo su instalación, pero por el contrario la imagen puede que pierda calidad a causa de las interferencias.

La sensibilidad a la luz de las cámaras con se mide mediante unidades de lux, las cuales determinan la cantidad mínima de luz necesaria para que la imagen pueda ser captada. Aproximadamente, 1 lux es equivalente a la luz que produce la llama de una vela. Para vigilar áreas con poca intensidad de luz, será necesario recurrir a cámaras cuya sensibilidad esté por debajo de 1 lux. Las cámaras de **visión nocturna** incorporan un sistema de infrarrojos que permite captar imágenes incluso en oscuridad total.

Las cámaras que denominamos **fijas** son aquellas que no se pueden mover y el área que captan es siempre el mismo. Por el contrario, las cámaras **móviles** son las que pueden enfocar hacia distintos puntos. Normalmente cuentan con un *joystick* que permita manejarlas desde el puesto de control donde se encuentra el vigilante. Otros modelos incorporan la posibilidad de programar el movimiento.

Existen también cámaras de **interior** y de **exterior**. Normalmente las cámaras de interior son móviles y están camufladas, de tal manera que un posible intruso no pueda esquivar el campo que ésta cubre. Las cámaras se suelen ocultar detrás de cristales espejo, de esta manera un posible intruso puede saber que hay una cámara pero no hacia donde está enfocando. Si lo que se pretende es cubrir una entrada, la cámara podrá ser fija.

Las cámaras de exterior suelen ser fijas y además no están camufladas, con lo que tienen un efecto disuasorio. Éstas se suelen colocar en el perímetro de las instalaciones de tal manera que éste se cubra completamente. Es recomendable que estas cámaras tengan además sistema de visión nocturna.

Estos sistemas deben además estar implantados, por lo menos, en las zonas más críticas del edificio. De esta manera si alguien accede a las instalaciones por una entrada que no hemos contemplado, será detectado al deambular por el interior de nuestras instalaciones y podremos actuar en consecuencia lo más rápidamente posible. Vamos a ver como proteger el interior del edificio en profundidad más adelante.

2.3.6 - Control de marcado de edificios y *Warchalking*

En el mundo *hacker* es una práctica común el marcado de fachadas para indicar que en determinado edificio es posible acceder a la red o a los datos corporativos mediante técnicas de *hacking*, sobre todo con la cada vez mayor implantación de tecnología inalámbrica (o *wireless*) para la transmisión de datos, y que permite el acceso a los datos en bruto e incluso la comunicación desde el exterior de la empresa.

Deberá estudiarse la fachada del edificio de forma que no encontremos signos de *Warchalking* u otro tipo de marcado sospechoso. El *Warchalking* es una técnica de marcado que mediante símbolos realizados con tiza en la fachada de un edificio indica que el edificio cuenta con una red *wireless* y las características de esta permiten la posibilidad de acceder a la red interna o la salida a la una red pública (conexión a Internet) a través de la red de la empresa. El *Warchalking* es extremadamente peligroso, pues expone las vulnerabilidades que un *hacker* haya encontrado en nuestra red a cualquier otro intruso que pase por delante de nuestro edificio.

La primera medida contra el marcado y el *Warchalking* es la implementación de plena seguridad en la red interna de la empresa, incluso evitando tecnologías que permitan el acceso indiscriminado a nuestros datos desde el exterior como las redes *wireless*. Como el tener plena seguridad informática es siempre un objetivo difícil de cumplir y debemos tener en cuenta que siempre será necesaria la vigilancia a posibles signos de marcado o *Warchalking*.

Los símbolos de *Warchalking* cambian con el tiempo e incluso son diferentes entre diferentes escuelas de *hackers*, por lo que deberemos sospechar de cualquier marca o símbolo que encontremos en el edificio y que pueda tener algún sentido. Si encontramos signos manifiestos de *Warchalking* tendremos que asumir que además del riesgo en la seguridad física que supone, tenemos un problema de seguridad informática, porque sabemos que alguien se ha preocupado de marcarnos como objetivo de ataques que son en teoría posibles.

2.4 - El interior del edificio

Vamos a ver los mecanismos de Seguridad Física con los que debemos contar en el interior del edificio. Normalmente las entidades cuentan con un centro computacional o centro de proceso de datos que es donde están ubicados los sistemas informáticos más sensibles, como pueden ser los *racks*(14) con los servidores o elementos de red, los terminales de gestión o las cintas con las copias de seguridad. Veremos más adelante la seguridad en estos centros y es donde haremos más hincapié, por ser el entorno directo de los sistemas informáticos.

(14) Armario o bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones. Sus medidas están normalizadas para que sea compatible con equipamiento de cualquier fabricante.

Sin embargo, es necesario que se cumplan unas medidas de Seguridad Física en el interior del edificio al completo, como pueden ser los pasillos o salas de reuniones, ya que si, por ejemplo, se produjera un incendio en una sala contigua a nuestro centro computacional, y aunque en ésta no tengamos ningún sistema informático ni crítico para

nuestra entidad, deberá ser sofocado de inmediato, en la propia sala, para evitar que se propague hasta los lugares donde sí tenemos estos sistemas.

Los elementos principales que se deben controlar en el interior del edificio son **intrusiones**, **incendios**, **inundaciones** y **polvo**. Otros factores, como humedad o temperatura, no es necesario desde el punto de vista de este trabajo que los tengamos controlados en todo el edificio, puesto que los podremos controlar de manera localizada en los lugares donde tengamos sistemas críticos, como el centro computacional. De esta manera, aplicaremos las ideas y conceptos que vamos a ver a continuación a la hora de proteger nuestro centro computacional.

2.4.1 - Intrusiones

Como hemos comentado anteriormente, aunque se tengan controlados todos los accesos al edificio, es necesario que se tenga conocimiento de quién está en nuestras instalaciones. Es posible que un intruso eluda alguno de nuestros controles de acceso o que un empleado esté en un área en la que no debe o haga algo indebido.

Para realizar este control se emplearán mecanismos vistos anteriormente como son detectores espaciales, barreras infrarrojas, detectores de rotura de vidrio, detectores perimetrales, detectores por presión y cámaras de vigilancia, además de vigilantes de seguridad. Vamos a ver los más adecuados para los tres tipos de zonas que encontramos en nuestras instalaciones: **zonas abiertas**, **zonas cerradas** y **zonas protegidas**.

a) Las zonas del edificio

i) Zonas abiertas
Las zonas abiertas son aquellas por las que hay gente en el desarrollo normal de nuestra actividad diaria, como son despachos, pasillos, puestos de trabajo, etc. En horas de trabajo es casi la totalidad del interior de nuestras instalaciones.

ii) Zonas cerradas
Son aquellas en las que no debe haber nadie. En el desarrollo normal de nuestra entidad y en horas de trabajo pueden ser almacenes cerrados, salas con servidores a los que no debe acceder nadie, etc. Sin embargo, fuera del horario de trabajo de nuestra entidad y en horas en las que ésta este cerrada debemos entender que, generalmente, el interior de nuestro edificio al completo es una zona cerrada.

iii) Zonas protegidas
Son las zonas especialmente sensibles dentro de nuestras instalaciones, como pueden ser el centro computacional. Además de las medidas de seguridad que adoptemos en el resto del edificio, estas zonas deben tener una seguridad añadida. Veremos medidas específicas más adelante.

b) Sistemas de control contra intrusiones

Como hemos visto anteriormente, para cubrir los accesos al edificio, estos dispositivos están conectados con una unidad de control y esta a su vez a los sistemas anunciadores.

Sin embargo, para cubrir el interior de nuestro edificio y cuando los empleados estén dentro de las instalaciones debemos llevar a cabo un control interno. Es decir, estos detectores deben estar controlados por un vigilante de seguridad dentro del propio edificio, ya que si se detecta una intrusión en una zona protegida se deberá controlar de inmediato. No tendría sentido que con empleados en el interior, porque haya habido un acceso irregular a una zona protegida, sonara una alarma en el exterior del edificio.

i) Detectores espaciales
Los detectores espaciales deben estar colocados en la práctica totalidad del interior de nuestras instalaciones pero solo activos en las zonas cerradas. No tiene sentido que en zonas abiertas, donde están nuestros empleados trabajando, estén éstos activos, ya que detectarían constantemente la presencia de gente.

ii) Barreras infrarrojas
Estos sistemas deben estar situados en puntos clave del interior de nuestras instalaciones, es decir, en puntos por los que un posible intruso deba pasar si deambula por nuestro edificio, así como en las puertas o puntos de acceso a las zonas protegidas. Solo deben estar activos en las zonas cerradas del edificio.

iii) Detectores de rotura de vidrio y detectores perimetrales
Generalmente estos sistemas solo deben estar protegiendo las zonas más sensibles de nuestras instalaciones. Los detectores perimetrales que protejan la puerta de nuestro centro computacional deben poder ser desactivados fácil y rápidamente para permitir acceder a estas zonas a los trabajadores cualificados.

iv) Detectores por presión
Aunque no es muy normal implantar este tipo de sistemas para proteger el interior del edificio, pueden ser totalmente válidos colocados en puntos clave de acceso a zonas protegidas o cerradas, así como en sitios por los que un posible intruso deba pasar si deambula por el interior de las instalaciones.

v) Cámaras de vigilancia
Con las cámaras de vigilancia se debe cubrir la práctica totalidad del interior de nuestras instalaciones. Deben estar colocadas en puntos estratégicos para emplear el mínimo número de cámaras en cubrir todo el edificio. Las cámaras deben estar operativas todo el tiempo, de esta manera controlaremos tanto las zonas cerradas como las zonas abiertas, además debemos hacer hincapié en cubrir con estos dispositivos las zonas más sensibles y los accesos a éstas. Como hemos mencionado anteriormente, las imágenes captadas por las cámaras deben estar monitorizadas en todo momento.

vi) Vigilantes de seguridad
Como acabamos de comentar, es importante que nuestro edificio esté custodiado por vigilantes de seguridad. Aunque podemos contratarlos como personal de la entidad, lo normal es que se contraten desde una empresa externa especializada. Se les deberá hacer firmar cláusulas, entre otras cosas, de confidencialidad, ya que esta personas tendrán acceso a la práctica totalidad de nuestros sistemas.

Dependiendo de las necesidades de nuestra entidad, lo normal es que los vigilantes de seguridad se encarguen de la entrada principal del edificio, verificando que los accesos a éste se realizan de la forma correcta. También deben controlar los sistemas de seguridad del edificio, tales como cámaras de vigilancia, sensores antiincendios, etc. Cuando el edificio está cerrado, se puede complementar la seguridad de éste con vigilantes.

2.4.2 - Incendios

Los incendios son una ocurrencia de fuego descontrolada y suponen una gran amenaza para cualquier entidad. Sus efectos son altamente destructivos, ya que las altas temperaturas que se alcanzan pueden dejar inservible cualquier sistema informático, documentos e incluso el edificio por completo. Se pueden producir fácilmente tanto en el interior como en el exterior de nuestro edificio (como ya hemos mencionado) y dado que los elementos que integran una oficina suelen ser altamente inflamables, su propagación es muy rápida.

Diferenciaremos entre los incendios que se pudieran producir y extender por el interior del edificio, los cuales veremos a continuación, y los que puedan afectar al centro computacional, que, como veremos más adelante, requieren unos sistemas de extinción diferentes. Esto es así por dos motivos, el primero es que el fuego se alimenta de materiales distintos, componentes electrónicos mayormente. El segundo es que los equipos que tenemos en nuestro centro computacional, como servidores o PC´s, no pueden ser rociados con ciertos agentes extintores, como el agua, puesto que los dejaría igualmente inservibles.

La actividad de Protección Contra Incendios está regulada y legislada por el **Reglamento de Instalaciones de Protección Contra Incendios R.D 1942/1993, RIPCI** que define las exigencias que debe cumplir un sistema de protección contra incendios en cuanto a la instalación de equipos y componentes, a su mantenimiento, a la marca de conformidad de los equipos, así como a sus especificaciones.

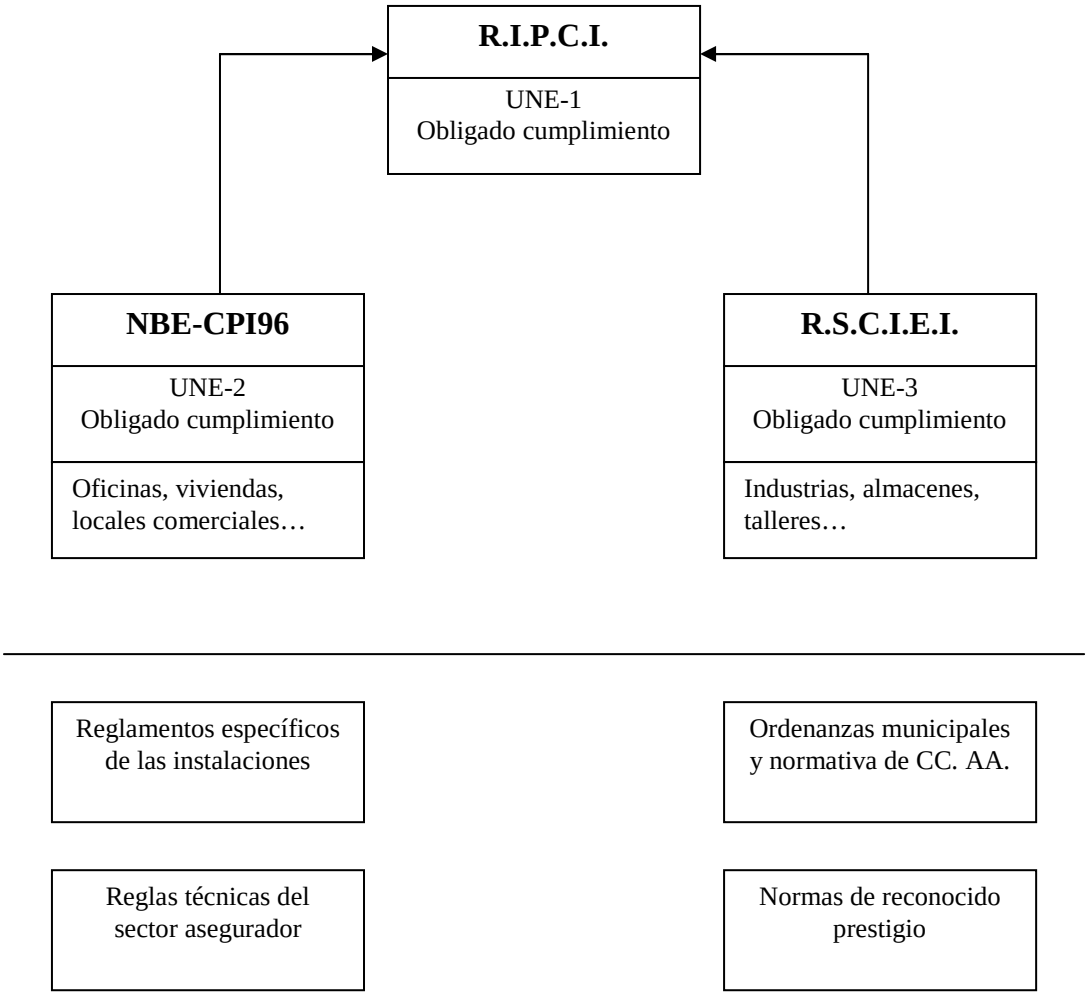
El reglamento se completa con la **Norma Básica de la Edificación, NBE-CPI/96, R.D 2177/1996,** y el **Reglamento de Seguridad Contra Incendios en Establecimientos Industriales, RSCIEI, R.D 781/2001**. Además, en el panorama reglamentario, existen normas específicas de instalaciones así como otras ordenanzas municipales, o normativas específicas autonómicas. En la mayoría de los casos el principal objetivo es el de poner a salvo al personal de la entidad, aspectos morales a parte, este no es un tema a tratar en este trabajo, por lo que trataremos en profundidad todas las normas y leyes que se deben cumplir con respecto a los incendios, a parte de que por su dispersión sería imposible abarcarlas todas en un trabajo de esta índole.

Esquema 2.8

Es muy conveniente que ciertos trabajadores de nuestra entidad estén adiestrados en todo lo referente a los incendios, como prevención, extinción, evacuación y planes de actuación. Empresas privadas y públicas ofrecen **cursos de formación antiincendios** pensados para este fin.

Esquema 2.8

Organización del sistema de protección contra incendios



a) Tipos de incendios

Lo primero que debemos conocer con respecto a los incendios es que los hay de distintos tipos, dependiendo del tipo de fuego del que estén alimentados. Existen varios tipos de fuegos. Podemos encontrar dos tipos diferentes de clasificaciones, la empleada en América, y la que vamos a mencionar a continuación, que es la manejada en Europa, Asia y Australia. Esto puede dar lugar a confusiones, sobre todo a la hora de emplear agentes extintores, ya que están diseñados especialmente para un tipo de fuego determinado, siendo inútiles, incluso peligrosos, si se utilizan en otros.

i) Tipo A
Son fuegos producidos por materiales sólidos como papel, madera y fibras y en general. Son todos aquellos que durante su ignición producen brasas o cenizas como residuo. Los materiales productores de fuego tipo A se caracterizan además por no tener desprendimientos de gases o vapores en su presentación natural.

ii) Tipo B
Los producidos por líquidos inflamables o sólidos licuables, siempre que tengan desprendimientos de gases. Algunos ejemplos son la gasolina, el petróleo, la pintura, aceites y algunas ceras o plásticos.

iii) Tipo C
Son los que implican gases inflamables, como el gas natural, el butano, el propano o el hidrógeno.

iv) Tipo D
Los que tienen su origen en cierto tipo de metales combustibles, tales como el zinc en polvo, el aluminio en polvo, el titanio o muchos otros metales cuando están reducidos a partículas muy finas. Tienen la peculiaridad de que su propia ignición produce el suficiente oxígeno como para mantener la combustión, además de que pueden reaccionar violentamente ante el agua u otros agentes extintores, por lo que se deben manejar con suma cautela.

v) Riesgo de electrocución (antes Tipo E)
Son los que implican materiales tipo A o B pero con la introducción de electrodomésticos, cableado o cualquier elemento sometido a una corriente eléctrica. Por lo que existe un riesgo de electrocución si se emplean agentes extintores conductores de la electricidad.

vi) Tipo F
Son los que implican grasas o aceites. Por definición son un subgrupo del tipo B, pero dado que las temperaturas que alcanzan los aceites o grasas en un incendio excede con mucho la de otros líquidos inflamables, hace inofensivos los agentes de extinción normales (en España el tipo F se incluye dentro del tipo B).

Una vez que conocemos los distintos tipos fuegos con los que nos podemos encontrar, vamos a ver como **prevenir**, **detectar**, **controlar** y **extinguir** un incendio que se produce en nuestras instalaciones. Llegado el caso se deberá hacer un estudio completo de cómo se ha originado, propagado, extinguido y qué daños a causado, entre otros

factores, para poder evitar que se pueda volver a producir o, por lo menos, estar mejor preparados.

Para ello y como veremos a continuación, será necesario instalar sistemas antiincendios. Por lo que se deben cumplir los requisitos expuestos en el **Real Decreto 1942/1993, de 5 de noviembre, por el que se aprueba el Reglamento de Instalaciones de Protección contra Incendios**. Aunque en España no está muy extendido el uso de los estándares para la definición y requisitos de los equipos y sistemas, el sector de la protección contra incendios es una excepción, por lo que vamos a mencionar las normas más relevantes, como son la **UNE-EN 54** y la **UNE 23007 de Sistemas de detección y alarmas de incendios** y la ya mencionada **UNE-EN 50136 Sistemas y equipos de transmisión de alarma**.

Es muy importante también que como parte de nuestros sistemas críticos y de vital importancia para la entidad, deben tener un funcionamiento ininterrumpido, por lo que deberán disponer en todo momento de un sistema auxiliar de alimentación eléctrica. Algunos de éstos dispositivos cuentan con baterías integradas, pero en cualquier caso, debemos cerciorarnos de que un corte en el suministro principal de energía no los deja fuera de servicio. La Norma **UNE 23007-4:1982. Componentes de los Sistemas de detección automática de incendios. Suministro de energía** habla sobre este aspecto.

b) Cómo prevenir un incendio

Para prevenir un incendio en el interior de nuestro edificio, la mayoría de las veces basta con seguir el sentido común. Para que el fuego comience es necesario que exista **oxígeno**, **una fuente de ignición** y **combustible**, por lo que si eliminàramos uno de estos factores sería imposible que se originara un incendio.

i) El oxígeno
Aunque, como veremos más adelante, existen sistemas de prevención y extinción de incendios que se basan en eliminar el oxigeno, por razones obvias es imposible que se elimine como medida preventiva en todo el interior de nuestras instalaciones.

ii) La fuente de ignición
Una fuente de ignición es cualquier elemento que puede causar un incendio. Dado que existen multitud de elementos inflamables en cualquier entidad, como son todos los derivados del petróleo, que actuarán como combustible, deberemos centrar nuestra atención en evitar este factor. Vamos a ver los distintos tipos.

ii.i) Llamas
Podría parecer que por ser el factor más evidente que puede producir un incendio, cualquier persona tendría sumo cuidado al manejarlas, sin embargo la mayor parte de las veces que se produce un incendio con una llama como fuente de ignición es por descuidos. Existen muchos elementos que la producen, como un mechero o un soplete, aunque el que hasta ahora más incendios ha provocado ha sido el tabaco.

Con la entrada en vigor de la **LEY 28/2005, de 26 de diciembre, de medidas sanitarias frente al tabaquismo** el 1 de enero de 2006, el tabaco debería dejar de ser un problema, puesto que está prohibido fumar en los puestos de trabajo.

Para evitar que una llama actúe como fuente de ignición en un incendio debemos evitar al máximo su utilización en el interior de nuestro edificio, controlar que todos nuestros empleados cumplen con la ley antitabaco y extremar las precauciones cuando se necesario el uso de elementos que la produzcan, tales como sopletes, mecheros, etc.

ii.ii) Instalaciones y aparatos eléctricos

Como ya hemos mencionado, existe un tipo de fuegos con gran riesgo eléctrico. En un momento dado puede que lo que provoque el incendio sean los propios sistemas eléctricos, puesto que estos dispositivos pueden alcanzar temperaturas muy altas, y en caso de avería o cortocircuito pueden provocar chispas que prendan los materiales cercanos.

Una instalación eléctrica envejecida, mal hecha o descuidada puede provocar un incendio fácilmente, por ello debemos verificar que el material aislante que cubre todas nuestras instalaciones está en perfecto estado, ya que una simple subida de tensión podría ser fatal. No debemos manipular las instalaciones eléctricas de nuestro edificio, en todo caso este cometido deberá ser llevado a cabo por personal cualificado.

Los aparatos eléctricos en mal estado también pueden provocar un incendio, por lo que nunca deben ser manipulados si no se sabe al cien por cien lo que se está haciendo y al mínimo síntoma de que pudiera fallar, como olor a quemado, calentamiento en exceso o humo, deberá ser desconectado de la red eléctrica inmediatamente.

ii.iii) Fuentes de calor

Las fuentes de calor intenso pueden también provocar un incendio. Las más comunes son las estufas o radiadores, por lo que si nuestro edificio cuenta con un sistema de calefacción o climatización, deberemos incluso prohibir su uso.

iii) El combustible

El combustibles es todo aquello que pueda arder, por lo que en un momento dado y con unas condiciones específicas, casi cualquier material puede ser un combustible. Además, como ya hemos mencionado, el amplio uso de materiales inflamables provenientes del petróleo, como son todos los plásticos y la gran mayoría de elementos sintéticos, hace que los elementos que componen el interior del edificio sean muy propicios para que se alimente el incendio. Sin embargo, existen materiales más resistentes al fuego que otros, de los cuales deberemos hacer uso en todo lo que nos sea posible. Vamos a ver unas pautas para dificultar al fuego abastecerse de combustible en nuestro edificio.

iii.i) Techos y suelos

Es muy normal que los edificios cuenten, especialmente en centros con un gran número de equipos eléctricos, con falsos techos y suelos para poder empotrar todos los cables y que de esta manera queden organizados y aislados. Es muy importante que estos falsos techos y suelos sean de material ignífugo o que por lo menos estén recubiertos con elementos que si lo sean. Existen en el mercado multitud de pinturas, polvos, barnices y

espumas con las que podemos cubrir cualquier material sin alterar su aspecto inicial y proporcionándole particularidades ignífugas. Si nos decantamos por esta opción, debemos verificar que los materiales que empleamos para tal fin cumplen con las normas UNE(15) e ISO para asegurarnos de su efectividad, a sí como de que no desprenden gases o sustancias tóxicas.

(15) Conforme a la normativa EN o UNE, se establece una clasificación de los materiales en función de su reacción ante cualquier acción térmica, basada en sus características de combustibilidad e inflamabilidad, que en el caso de un incendio sería su grado de combustión y su capacidad para propagar el mismo. Dicha clasificación abarca desde el nivel M-0, correspondiente a materiales incombustibles, hasta el nivel M-4 correspondiente a materiales altamente inflamables.

iii.ii) El mobiliario
Entendemos por el mobiliario todo lo que compone el interior del edificio, desde sillas y mesas hasta armarios, barandillas, escaleras o elementos decorativos, como cuadros o carteles. Al igual que los falsos techos y suelos, deberemos procurar que sean de materiales ignífugos, o por lo menos que no estén fabricados con materiales inflamables, como los plásticos y derivados del petróleo. Aunque lo veremos más adelante en profundidad, hay que mencionar ahora que los armarios donde se guarde información sensible para nuestra entidad, cintas con las copias de seguridad o cualquier elemento de valor, deberán ser especialmente resistentes al fuego.

iii.iii) Limpieza
Es muy importante que los pasillos y despachos estén libres de basuras y desperdicios, especialmente de papeles o plásticos, ya que estos arden con suma facilidad. Debemos hacer hincapié en este aspecto ya que es normal encontrarnos con papeleras llenas de papeles o desperdicios tirados en el suelo o, incluso, acumulados en falsos suelos o detrás de mubles. Debemos velar por que el interior de nuestro edificio esté perfectamente limpio.

iii.iv) Materiales inflamables
Si disponemos de un generador eléctrico de emergencia en nuestro edificio, deberemos tener almacenado su combustible. Como ya hemos visto, este suele ser gasóleo o gasolina. Estas sustancias son altamente inflamables, por que se deberán tomar unas medidas especiales. La Norma **UNE-EN 60079-10** nos habla de cómo clasificar los distintos lugares dependiendo de las sustancias de las que disponga en su interior, y según la clasificación en la que nos encontremos, deberemos actuar de una manera u otra. Otro factor importante es la salida de gases del generador, puesto que éstos están considerados como elementos inflamables, se deberá disponer, por tanto, de un sistema antiincendio para fuegos del tipo C.

c) Cómo detectar un incendio

La detección del incendio es sumamente importante, ya que si este se llegará a producir, deberemos detectarlo para que se activen nuestros sistemas de extinción. Cuanto más sensibles y localizados sean sensores, más eficaces serán nuestros sistemas de extinción, y por tanto, antes conseguiremos sofocar el incendio.

Existen multitud de sistemas de detección de incendios. Los hay automáticos y manuales y pueden estar conectados a los sistemas de alarma generales del edificio o pueden constituir un sistema por si mismos. La unidad de control de este sistema, sea compartida o no, debe poder realizar unas funciones específicas, como es activar los sistemas de extinción y comunicar inmediatamente a los bomberos que se está produciendo un incendio. Además, lo normal es que puedan realizar cualquier tarea para la que hayan sido programados, como por ejemplo, cortar la corriente eléctrica del edificio, aislar zonas con el fin de evitar que se extienda el incendio, encender el alumbrado de emergencia (consultar **UNE 50172:2005. Sistemas de alumbrado de seguridad)**, activar una alarma sonora, etc.

En el caso de los detectores de incendios, es especialmente necesario que la unidad de control identifique donde se encuentra el detector que ha activado la alarma, de esta manera será más sencillo localizar el fuego y proceder a su extinción.

Los detectores de incendios y como todos los elementos que componen nuestro sistema antiincendios, precisan de un mantenimiento especial que veremos más adelante.

i) Sistemas de detección manuales

Es muy probable que si se originara un incendio en nuestras instalaciones en horas de trabajo, los primeros en detectarlo fueran nuestros propios empleados. Esto es así porque el fuego produce una gran cantidad de humo y un olor a quemado muy característico. Es por ello que debe existir algún sistema que permita a los trabajadores avisar de la situación. Podemos decir entonces que los detectores manuales no son detectores en sí, si no **avisadores** que permiten a los empleados que han detectado el incendio alertar sobre éste.

Los avisadores, también llamados pulsadores, deben estar colocados en la pared, protegidos, para evitar su accionamiento involuntario, por cajas de cristal inastillable fácilmente rompible. Colocados en los pasillos de cada planta, al menos uno cada 25 metros y siembre debe haber uno a la vista. Deben estar también colocados en las habitaciones o salas donde se guarden materiales inflamables, como pudiera ser la gasolina de nuestro generador de electricidad auxiliar. Además, todos los avisadores deben estar perfectamente señalizados por carteles homologados.

ii) Sistemas de detección automáticos

Existen múltiples tipos de detectores de incendios, y al igual que los detectores de intrusiones vistos anteriormente, emplean tecnologías diferentes, por lo que es necesario conocer las carencias de unos para suplirlas con otros. Además, cuantos más detectores tengamos, más localizado será el incendio, y por lo tanto, más sencilla será su extinción. Los tipos de detectores más empleados son los de **temperatura** o **térmicos** y los **detectores de humos**, **ópticos** e **iónicos**. Vamos a ver cada uno de ellos y dónde debemos ubicarlos.

ii.i) Detectores de temperatura o térmicos

Estos dispositivos son capaces de detectar la temperatura y, en base a ésta, activar la señal de alarma. Existen tres tipos, **de temperatura fija**, ***velocimétricos*** y **combinados**.

ii.i.i) Detectores de calor de temperatura fija
Estos detectores activan la alarma al detectar una temperatura prefijada, dependiendo del modelo y la tecnología que empleen, pueden programarse para cambiar la temperatura a la que queremos que activen la señal de alarma o no. Es común que estos detectores tengan una pieza de un material metálico que se funde a una temperatura determinada y activan la alarma. Este tipo de dispositivos quedan inoperantes y deben reemplazarse tras su accionamiento, por lo que es muy importante consultar las características técnicas de cada modelo en concreto.

ii.i.ii) Detectores de calor *velocimétricos*
Los detectores de calor *velocimétricos* basan su funcionamiento en el cambio de temperatura que se produce a su alrededor. Cuando la temperatura aumenta a un ritmo muy elevado, generalmente a 8,3º C por minuto, activan la señal de alarma. Este tipo de detectores están indicados para fuegos que se producen de manera rápida y violenta.

ii.i.iii) Detectores de calor combinados
Este tipo de detectores combinan las dos tecnologías vistas anteriormente, la de los detectores de calor de temperatura fija y la de los detectores de calos *velocimétricos*. Éstos ofrecen mayores ventajas que los anteriores, ya que el elemento *velocimétricos* ofrece una respuesta más rápida ante un fuego violento y el de temperatura fija detectará fuegos lentos.

ii.ii) Detectores de humo iónicos
Este tipo de detector es más barato que el óptico y puede detectar partículas que son demasiado pequeñas como para influir en la luz, de entre 0,01 y 0,3 micras de tamaño. Está compuesto por una pequeña cantidad del isótopo radioactivo, americio-241, que emite radiación alfa. La radiación pasa a través de una cámara abierta al aire en la que se encuentran dos electrodos, permitiendo una pequeña y constante corriente eléctrica. Si entra humo en esa cámara se reduce la ionización del aire y la corriente disminuye o incluso se interrumpe, con lo que se activa la alarma.

Estos detectores son especialmente adecuados para detectar vapores y gases, así como las partículas generadas en fuegos rápidos, los que generan gran cantidad de llama desde el principio, por lo que son los indicados para lugares donde haya material inflamable, como gasolina y derivados del petróleo, pinturas, disolvente, gas butano, propano, etc., así como madera, lana, cuero o cables eléctricos. Factores como la suciedad, el polvo, la humedad, la altura, los aerosoles o las variaciones en la corriente eléctrica pueden alterar su funcionamiento, pudiendo provocar falsas alarmas.

ii.iii) Detectores de humo ópticos
Existen dos tipos de detectores ópticos, según detectes el humo por oscurecimiento o por dispersión del aire en un espacio. A efectos prácticos, los dos tipos son casi idénticos y especialmente indicados para detectar humos de fuegos lentos, esto es, los que producen mucho humo desde el principio.

ii.iii.i) De rayo infrarrojo o *por oscurecimiento*

Compuestos por un dispositivo emisor y otro receptor. Cuando se oscurece el espacio entre ellos debido al humo, sólo una fracción de la luz emitida alcanza al receptor, provocando que la señal eléctrica producida por éste sea más débil y se active la alarma. Aunque son indicados para lugares amplios, su uso no está muy extendido ya que no se deben emplazar en lugares con corrientes de aire o ventilación y requieren un mantenimiento para alinear emisor y receptor.

ii.iii.ii) De tipo puntual o *por dispersión*
En este tipo de detectores, un emisor de luz y un receptor se encuentran alojados en la misma cámara, de tal manera que la luz emitida por el emisor es tan débil que el receptor no es capaz de detectarla. Cuando dicha cámara se llena de humo, este refleja la luz, por lo que hay un aumento de cantidad de luz en la cámara y el receptor la detecta, es entonces cuando se activa la señal de alarma. Detecta partículas de entre 0,3 a 10 micras de tamaño y es el tipo de detectores más empleados en oficinas, tiendas y fábricas. Aunque su funcionamiento se puede ver alterado por polvo, suciedad o pequeños insectos, pueden ser regulados para evitar fallos y pueden avisar cuando estén muy sucios, además no les afecta ni la altura ni la humedad. Se suelen combinar con detectores iónicos.

iii) Dónde y cómo ubicar los detectores
Dado que el aire caliente tiende a subir, los detectores deberán estar situados en los techos o las partes más altas de las paredes. Aunque debemos seguir las especificaciones de cada modelo en concreto, vamos a ver unas pautas generales que se deben seguir a la hora de colocar nuestros detectores con el fin de que sean lo más eficaces y precisos posible.

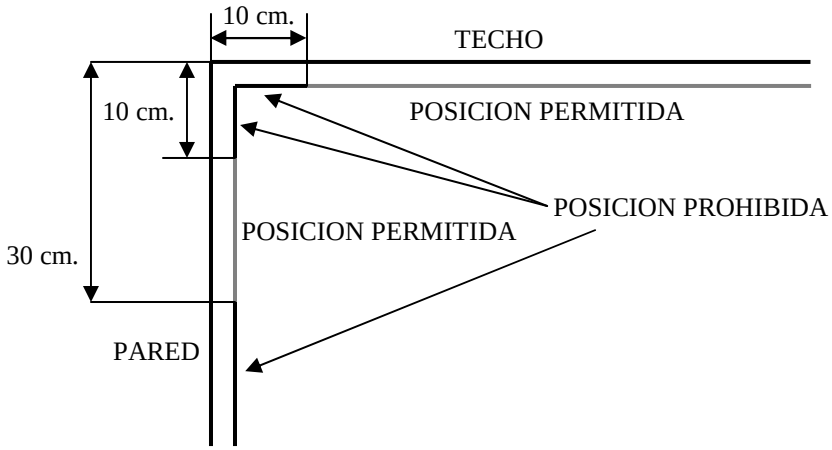
Si los colocamos en el techo, deberemos dejar una distancia hasta la pared más cercana de, por lo menos, 10 centímetros. Si por el contrario los colocamos en la pared, deberá haber una distancia desde el detector hasta el techo no inferior a 10 centímetros y no superior 30 centímetros.

Para conocer la distancia que debemos dejar entre detectores, debemos saber cuál es el área que son capaces de cubrir. Existen factores que pueden alterar esta distancia, como son la estructura del techo, puede ser a dos aguas, liso o en dientes de sierra, o elementos que puedan interferir en el funcionamiento de los detectores, como vigas, viguetas o salientes.

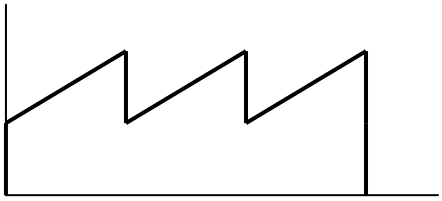
Esquema 2.9

Esquema 2.9

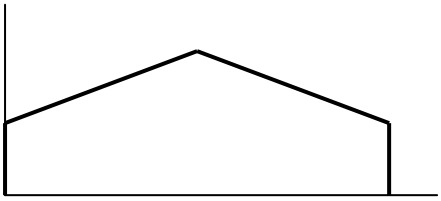
Ubicación de los detectores de incendios



Distintos tipos de techos



Techo en dientes de sierra



Techo a dos aguas

En el caso de los detectores de humo, además de estas consideraciones, se tendrá que tener muy presente las posibles corrientes de aire, así como su temperatura, sobre todo si los detectores están ubicados en el techo.

Si existe una corriente de aire que arrastra el humo impidiendo que éste pase por nuestros detectores, éstos no detectarán el posible incendio.

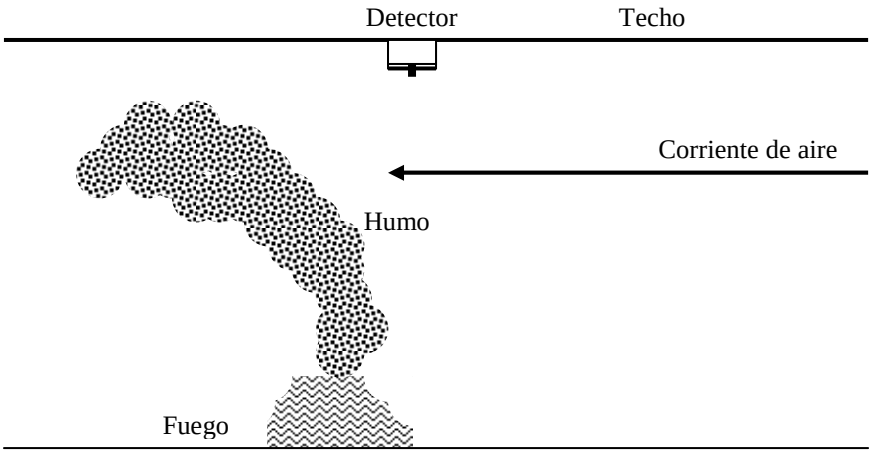
Por otro lado, si nuestros detectores están ubicados en el techo y éste está sobrecalentado por, por ejemplo, las radiaciones del sol, se generará una capa de aire más caliente que el humo pegada al techo que impedirá que éste llegue hasta los detectores. Si por el contrario el techo está demasiado frío por, por ejemplo, un conducto de aire acondicionado, el humo se enfriará al llegar a la zona de aire frío y caerá hacia abajo antes de llegar a los detectores.

Esquema 2.10

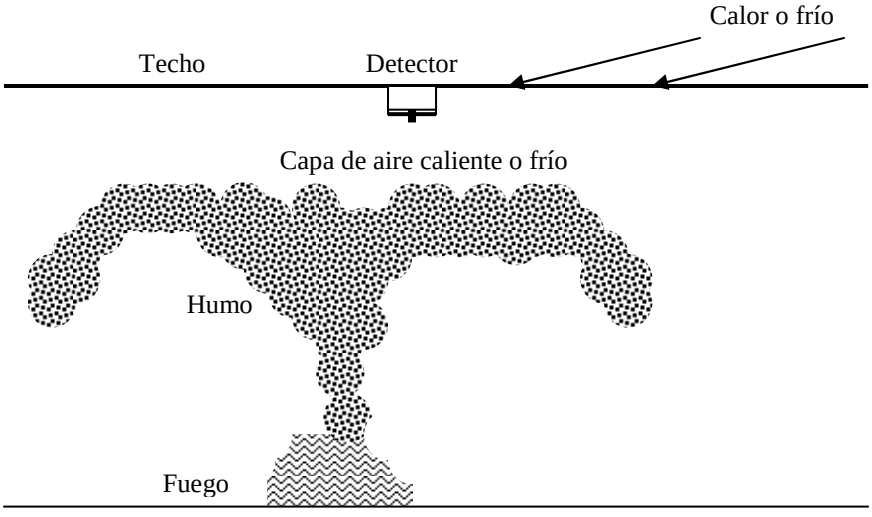
Esquema 2.10

Factores a tener en cuenta con detectores de humo

a) Corrientes de aire



b) Techo sobrecalentado demasiado frío



d) Cómo controlar un incendio

Para minimizar los daños que nos pueda causar un posible incendio, es necesario que el fuego no pueda avanzar por todo nuestro edificio. Como hemos comentado antes, un incendio que se inicia en una sala o un pasillo, puede afectar en poco tiempo a todas las instalaciones. Es por ello que debemos delimitar unas zonas dentro del edificio de tal manera que el fuego no pueda atravesarlas. De esta manera, un incendio que se inicia en una sala, solo podrá afectar a la zona en la que dicha sala se encuentra, pero no al resto. Una buena manera de dividir el edificio es en base al tipo de fuego que puedan crear los elementos que se encuentran en cada zona, de esta manera podremos usar medios de extinción específicos para cada uno de los sectores de incendio.

Para ello se debe realizar un estudio con el objetivo de conocer como delimitar estas zonas lo más eficientemente posible. A estas zonas se las denomina **sectores de incendio**. De tal manera, se puede definir un sector de incendio como aquella zona delimitada que es capaz de garantizar el confinamiento del fuego durante un tiempo determinado con el fin de retrasar su propagación a otras zonas del edificio. Normalmente, las zonas más críticas del edificio, como el centro computacional, deberán ser sectores de incendio, así como el edificio al completo, para evitar que el fuego se propague hasta las instalaciones colindantes.

Para conseguir ese objetivo, los sectores de incendio deben estar delimitados por paredes, puertas y techos que mantengan un **valor de resistencia al fuego** (**RF**) durante un tiempo determinado. De la misma manera que los elementos de la estructura del edificio, como vigas, pilares o forjados, alcancen un **grado de estabilidad al fuego** (**EF**) que les permita soportar las altas temperaturas del incendio sin llegar al colapso.

El tiempo (**t**) que define en minutos los valores de RF y EF debe ser uno de los siguientes valores normalizados: 15, 30, 45, 60, 90, 120 o 240. Así, el comportamiento al fuego de los elementos que delimiten los sectores de incendios se determina según pruebas de laboratorio en las que elementos similares son sometidos al calor, alcanzando una temperatura prefijada en normas específicas. Si estos elementos alcanzan uno de los tiempos indicados anteriormente, por ejemplo 60, diremos que tiene un valor EF de 60, lo que quiere decir que durante 60 minutos puede soportar las altas temperaturas sin perder sus cualidades.

El factor observado para los elementos estructurales a los que se les aplica el EF es que **mantengan su capacidad de carga**. Para los elementos empleados en delimitar sectores de incendios, como puertas, techos o paredes, a los que se les aplica el RF, además de observar que mantengan su capacidad de carga, se verifica que **no emita gases inflamables por la cara no expuesta al fuego**, **no emita gases calientes ni llamas por la cara no expuesta al fuego** y que **la temperatura de la cara no expuesta al fuego sea inferior a la que establece la Norma UNE-23.093 Ensayo de resistencia al fuego de las estructuras y elementos de la construcción.** Otra norma que debemos consultar es la **UNE-23.802 Ensayo de resistencia al fuego de puertas y otros elementos de cierre de huecos.**

e) Cómo extinguir un incendio

Como ya hemos mencionado, para que se produzca o tenga continuidad un incendio se deben de dar unos factores básicos, como son una llama o calor, combustible y oxígeno, por lo tanto, para extinguirlo se debe actuar contra alguno de estos factores. Existen distintas **técnicas** para que alguno de estos factores no se dé en el incendio y por tanto se extinga. Para ello, disponemos de unos **agentes extintores** que variarán y tendrán un cometido distinto dependiendo del tipo fuego queramos extinguir. Para poder aplicar estos agentes extintores vamos a disponer de unos **sistemas de dosificación**. Vamos a ver todo esto en profundidad.

i) Técnicas

Vamos a ver cada una de las distintas técnicas que podemos aplicar a un incendio para extinguirlo. Como ya hemos mencionado, dependiendo del tipo de fuego deberemos aplicar unas u otras.

i.i) Enfriamiento
Como su nombre indica, consiste en eliminar la fuente de calor o rebajarla a determinados valores suficientemente bajos como para que el incendio no se desarrolle. Es la técnica más empleada, normalmente en fuegos tipo A y de riesgo eléctrico.

i.ii) Eliminación del combustible
Consiste en eliminar el combustible que alimenta un incendio. No es muy normal que en un incendio nos paremos a separar los materiales que lo rodean para que no ardan, por lo que se emplea con incendios provocados por un escape de gas o de líquidos inflamables cortando la llave de paso que alimenta las tuberías dañadas. Con los demás tipos de fuegos puede ser una medida de precaución, retirando materiales cercanos al fuego para evitar que se reaviven las llamas, una vez que hemos controlado el fuego.

i.iii) Disolución del combustible
En ocasiones, y normalmente con fuegos tipo B, no es necesario llegar a la eliminación total del combustible para que cese el proceso de combustión. Basta diluirlo hasta valores adecuados por debajo de los cuales la cantidad de comburente sea lo suficientemente pobre como para que no se inicie el incendio.

i.iv) Separación de comburente y combustible
Consiste en colocar una capa física, con una agente extintor, como espuma o como una simple manta, entre el combustible y el comburente, material que ya está ardiendo. Si estos dos elementos están separados, el combustible no arderá y el incendio podrá ser controlado.

i.v) Supresión del oxígeno o sofocación
Dado que el oxígeno es necesario para que exista el fuego, la supresión de éste hará que el fuego cese. Existen múltiples maneras de suprimir el oxígeno de una zona, pero por razones obvias, sólo podrá ser aplicado en zonas que estén totalmente desocupadas.

i.vi) Reacciones químicas
Existen ciertos polvos que actúan como catalizador, inhibiendo la reacción de combustión.

Para fuegos tipo D, dado que son extremadamente virulentos y de muy diversa naturaleza, existen ciertos compuestos químicos ideados para cada caso concreto. Puesto que en los centros que vamos a estudiar en este trabajo no es normal que haya el tipo de metales que puedan provocar fuegos tipo D, no vamos a profundizar más en estos casos.

ii) Agentes extintores

Como ya hemos mencionado, puede que para sofocar algunos incendios baste con cerrar una llave de paso o echar una manta por encima. No obstante, lo normal es que sea preciso emplear agentes extintores para que, mediante alguna de las técnicas vistas anteriormente, el incendio sea sofocado. Dado que existen multitud de agentes extintores, vamos a ver los más usuales y representativos.

ii.i) Agua
Posiblemente el agente más universal y barato. Apaga el fuego por enfriamiento, absorbiendo el calor del fuego para evaporarse. La cantidad de calor que absorbe es muy grande y en general es más eficaz si se emplea pulverizada, ya que se evapora más rápidamente, con lo que absorbe más calor. Además, el agua cuando se vaporiza aumenta su volumen 1600 veces.

Es especialmente eficaz para apagar fuegos del tipo A, ya que apaga el fuego y enfría las brasas. No debe emplearse ni en fuegos tipo B ni en fuegos tipo C, a no ser que esté debidamente pulverizada. Es conductora de electricidad, por lo que tampoco debe emplearse en fuegos con riesgo de electrocución, salvo que se emplee debidamente pulverizada, en tensiones bajas y respetando las debidas distancias. Jamás debe emplearse en fuegos tipo D, ya que por reacción química, puede provocar explosiones.

ii.ii) Espumas
Es una emulsión de un producto *espumógeno* en agua. Básicamente apaga por sofocación, al aislar el combustible del ambiente que lo rodea, ejerciendo también una cierta acción refrigerante, debido al agua que contiene. También se puede emplear para crear una capa entre el fuego y el combustible, de tal manera que impida el contacto entre ambos.

Se utiliza normalmente en fuegos del tipo A, B y C. Es conductora de la electricidad, por lo que no debe emplearse en presencia de corriente eléctrica. Tampoco es adecuado emplearlo en fuegos tipo D.

ii.iii) Polvos químicos secos
Son polvos de sales químicas de diferente composición, capaces de combinarse con los productos de descomposición del combustible, paralizando la reacción de combustión. Existen dos tipos, **polvos BC** y **polvos ABC**. Las letras nos indican para qué tipo de fuego están indicados.

ii.iii.i) Polvos normales o polvos BC
Los polvos químicos secos normales son sales de sodio o potasio, perfectamente secas, combinados con otros compuestos para darles fluidez y estabilidad. Son apropiados para fuegos del tipo B y del tipo C.

ii.iii.ii) Polvos polivalentes o polvos ABC
Los polvos químicos secos polivalentes tienen como base fosfatos de amonio, con aditivos similares a los de los anteriores. Además de ser apropiados para fuegos de los tipos B y C, lo son para los del tipo A, ya que se funden recubriendo las brasas con una película que las sella, aislándolas del aire.

No son tóxicos ni conducen la electricidad a tensiones normales, por lo que pueden emplearse en fuegos en presencia de tensión eléctrica (La tensión máxima sobre la que pueden ser rociados debe estar indicada). Su composición química hace que contaminen los alimentos y pueden dañar por abrasión mecanismos delicados.

ii.iv) Gases inertes
Apagan el fuego reduciendo el nivel de oxígeno por debajo del porcentaje necesario para que éste se alimente. El fuego necesita una concentración mínima de oxígeno en el ambiente de entre el 14 y el 16% para mantener la combustión, este tipo de gases la dejan en torno a un 12%, dependiendo de la concentración de gas empleado. Sin embargo, el ambiente sigue siendo respirable, aunque debido a la falta de oxígeno, aumentará el ritmo cardiaco de los presentes y si la concentración del gas empleado deja el nivel de oxígeno por debajo del 12%, se deberá evacuar la sala en un tiempo menor de 30 segundos. El nivel de oxígeno en áreas ocupadas nunca debe ser menor del 10%.

Durante la descarga de estos gases se mantiene una buena visibilidad. No son tóxicos, no dañan la capa de ozono y no provocan el efecto invernadero.

Los más empleados son el argón, la mezcla de argón y nitrógeno y el dióxido de carbono, siendo las características de todos ellos muy similares. Se pueden emplear en los fuegos de los tipos A, B y C, pero están especialmente indicados para los que implican riesgo de electrocución, ya que no son conductores. Al no dejar residuos se pueden emplear para sofocar incendios donde el material sea especialmente sensible. Por ello, veremos en profundidad estos agentes extintores cuando hablemos del centro computacional.

ii.v) Halones
Los halones son hidrocarburos halogenados (*bromofluorocarbonados*) que tienen la capacidad de extinguir el fuego mediante la captura de los radicales libres que se generan en la combustión. Hasta que se determinó que producían daños a la capa de ozono, fueron los productos extintores más eficaces para combatir el fuego, ya que, sumado a su alto poder de extinción, fácil proyección y pequeño volumen de almacenamiento, presentan una toxicidad muy baja, buena visibilidad y no provocan daños sobre los equipos electrónicos y eléctricos sobre los cuales se descargan, al no dejar residuo. Los más utilizados como agentes extintores fueron el halón 1301 para instalaciones fijas y el halón 1211 para extintores portátiles.

El Reglamento (CE) 2037/2000 mantiene la prohibición de la producción y, además, afecta al uso de los halones 1301 y 1211, de forma que los sistemas de protección contra incendios y los extintores de incendios que contengan halones deberán haber sido retirados del servicio antes del 31 de diciembre de 2003 salvo para unos usos críticos, como en cabinas de aviones o vehículos de guerra. Es por ello que se han desarrollado

unos gases como alternativa a su uso, los llamados gases halogenados, que veremos a continuación.

ii.vi) Gases halogenados

Estos productos extintores son compuestos químicos orgánicos que en su composición contienen átomos de CI, F o I, solos o en combinación. Si bien son menos efectivos que los halones, por lo que las concentraciones de agente extintor son mayores, su forma de actuar es similar y son en general gases licuados o líquidos compresibles que se *sobrepresurizan* con nitrógeno para aumentar la velocidad de descarga. Como inconveniente cabe mencionar que algunos de ellos también deberán reemplazarse en el futuro por afectar a la capa de ozono, aunque lo hacen en menor medida que los halones. Este tipo de agentes extintores son especialmente propicios para el centro de computación y en general para proteger equipos electrónicos o material delicado. Vamos a ver los más empleados.

ii.vi.i) HFC-227ea

Este agente es apto para la protección de la mayoría de los riesgos donde anteriormente se tenía que aplicar el Halón 1301. Una vez descargado, el HFC-227ea extingue rápidamente el fuego minimizando los daños a la propiedad y a los equipos de alto valor, asegurando asimismo la total seguridad a las personas. Además no deja residuos para su limpieza posterior, por lo que permite continuar de inmediato las actividades

El HFC-227ea usa un mecanismo diferente para la extinción que el Halón 1301, éste extinguía el fuego por reacción química eliminando radicales libres, mientras que el HFC-227ea actúa físicamente por absorción de calor. Es seguro para las personas porque no sólo extingue el fuego sin reducir la cantidad de oxígeno, sino que no resulta tóxico en las concentraciones específicas de utilización. Por estos motivos, HFC-227ea es idóneo para la protección de ambientes ocupados normalmente por personas.

Está indicado para fuegos del tipo A, del tipo B y en los que existe riesgo de electrocución, ya que no es conductor de la electricidad. Se debe almacenar a una temperatura de entre 0 y 50ºC y la altura máxima hasta el suelo debe ser de 3,5 metros.

ii.vi.ii) HFC-23

El HFC-23 extingue los incendios principalmente por absorción de calor y también, en menor proporción, químicamente por eliminación de radicales libres de la zona del fuego. Debido a su presión de vapor natural, el HFC-23 no requiere presurización con nitrógeno.

El HFC-23 es totalmente seguro para las aplicaciones en áreas ocupadas. La mayoría de los sistemas de HFC-23 se diseñan con una concentración de 16%, siendo el NOAEL[(16)] de este agente extintor del 30%. Un margen de seguridad tan amplio lo tienen muy pocos agentes extintores disponibles en el mercado.

[(16)] La concentración de diseño tiene que estar por debajo del NOAEL (*No Observed Adverse Effect Level*), que es la concentración hasta la cual no se observa ningún efecto adverso.

Está indicado para fuegos de los tipos A, B y en los que exista riesgo de electrocución, ya que tampoco es conductor de la electricidad. El HFC-23 no deja residuos ni durante

la extinción del incendio ni después de una descarga accidental. Es especialmente útil para áreas que requieren almacenamiento a temperaturas bajas, hasta -40°C, y locales con techos de hasta 7,5 m de altura o incluso más altos.

ii.vi.iii) HCFC-mezcla A
Está compuesto por una mezcla de hidrocarburos halogenados (HCFC) y un aditivo *detoxificante*, en condiciones de reducir drásticamente la cantidad de productos de descomposición que se forman en presencia de la llama. Es un gas incoloro, no es conductor de la electricidad y tiene una densidad unas 6 veces mayor que la del aire. Extingue incendios principalmente físicamente mediante la absorción de calor en el riesgo pero también actúa químicamente

Es un agente extintor pensado para sustituir al Halón 1301 ya su empleo en los sistemas antiincendio existentes proyectados para el Halón 1301 no requieren modificaciones sustanciales. En las aplicaciones más comunes es necesaria una cantidad en peso de HCFC-mezcla A mayor del 10% con respecto al Halón 1301 y, por consiguiente, en la mayoría de los casos es posible instalarlo en los sistemas ya existentes sin modificar las tuberías diseñadas pare el Halón 1301.

HCFC-mezcla A es apto para fuegos de tipo A, tipo B y en los que exista riesgo de electrocución, por no ser conductor. Se distribuye fácilmente a temperaturas bajas y los niveles de toxicidad permiten su uso en áreas normalmente ocupadas para las aplicaciones más comunes.

El impacto medioambiental global es extremadamente bajo, pero el potencial de agotamiento de ozono no llega a ser cero, por lo que los HCFC están incluidos en el Reglamento 2037/2000 y está prohibido el suministro para nuevas instalaciones dentro de la CE, estando permitida su utilización de forma controlada y estando prevista su eliminación en el futuro.

ii.vi.iv) FS 49 C2
FS 49 C2 se desarrolló para reemplazar el halón 1301, ofreciendo propiedades físicas y características de extinción parecidas aunque con un impacto ambiental mínimo. Es una mezcla de gases basada principalmente en el HFC-134a. Al igual que el HCFC-mezcla A, se requieren unos mínimos ajustes técnicos en las instalaciones del halón 1301 para poder emplearlo, así como aumentar ligeramente la capacidad del lugar de almacenamiento del gas, ya que se requiere un 40% más de volumen de extinción.

Las concentraciones de trabajo no representan peligro para los humanos. Es un agente limpio, que se descarga rápidamente por lo que limita los daños causados por el fuego y que no causa daños tras su descarga al contenido de los edificios. No tóxico ni daña la capa de ozono. Indicado para fuegos del tipo A, del tipo B y los que conllevan riesgo de electrocución, por no ser conductor.

ii.vi.v) HCFC-mezcla C
Es un agente extintor pensado para sustituir al Halón 1211. Es un agente limpio aplicable a extintores portátiles y en las aplicaciones locales. Está compuesto por una mezcla de hidrocarburos halogenados y un aditivo detoxificante que reduce la cantidad de productos de descomposición que se forman en presencia de la llama.

El HCFC-mezcla C no supone un riesgo para las personas por si mismo, aunque los productos de descomposición pueden suponer un riesgo. Por ello se incorpora un aditivo detoxificante que al estar expuesto a las altas temperaturas de las llamas reduce los humos ácidos tóxicos e inertiza los compuestos halogenados más tóxicos. Daña la capa de ozono a un nivel despreciable y no provoca efecto invernadero. Es efectivo para fuegos de los tipos A, B, C y os que implican riesgo de electrocución.

ii.vii) Extintores específicos para fuegos tipo D
Como ya hemos mencionado anteriormente, los fuegos tipo D son de muy diversa naturaleza, por lo que para cada caso concreto es necesario emplear un agente extintor específico. La única manera de aplicar estos agentes es directamente sobre el fuego a tratar y desde un extintor portátil (los veremos a continuación) adecuado.

Hay que decir también, que si empleamos dos tipos distintos de agente extintor en la misma zona, debemos asegurarnos de que son totalmente compatibles, ya que muchos de estos compuestos pueden reaccionar entre sí produciendo efectos no deseados.

iii) Métodos de aplicar los agentes extintores

Básicamente, existen dos sistemas para aplicar los agentes extintores vistos anteriormente, los **manuales** y los **automáticos**. Como veremos a continuación, su manera de actuación es totalmente distinta, y existen para cada tipo unos agentes extintores específicos. Los extintores manuales son portátiles se emplean directamente contra el fuego, mientras que los automáticos son fijos y suelen actuar rociando por completo la zona de agente extintor.

iii.i) Métodos manuales
Los métodos manuales de aplicación del agente extintor son aquellos que necesitan ser manejados por un individuo. Están pensados para que ante un incendio, el personal de la entidad, incluso antes de que se active la alarma antiincendios, pueda emplearlos **rápida y directamente** contra el fuego que se está produciendo. Dado que precisan la actuación de una persona, deberán estar correctamente señalizados de forma tal que resulten fácilmente visibles. Las señales serán las definidas en la Norma **UNE 23 033** y su tamaño será el indicado en la Norma **UNE 81 501**. Vamos a ver los dos tipos existentes, los **extintores portátiles** y las **bocas de incendio**.

iii.i.i) Extintores portátiles
Los extintores portátiles son artefactos que consisten básicamente en tres partes: una bombona o cilindro de acero que contiene el agente extintor, una válvula para su apertura y una boquilla para dirigir la salida de este agente extintor. El artefacto en sí se traslada hasta el lugar donde se está produciendo el incendio para su utilización. Es por ello que si la masa del conjunto sobrepasa los 20 Kilogramos, deberá constar de un medio de transporte sobre ruedas incorporado al extintor. Las características, criterios de calidad y ensayos de los extintores móviles se ajustarán a lo especificado en el **Reglamento de Aparatos a Presión** del Ministerio de Industria y Energía así como en las normas **UNE 23-110/75**, **UNE 23-110/80** y **UNE 23-110/82**.

Normalmente los extintores portátiles se clasifican según el agente extintor del que están provistos. Como veremos más adelante, los agentes extintores pueden ser de cualquiera de los tipos antes mencionados: agua, espumas, CO_2, gases inertes, gases halogenados y los más comunes, polvos químicos secos.

Dado que al activar la válvula el agente extintor sale a presión, otra manera de clasificar los extintores portátiles es dependiendo de si el agente extintor provoca esa presión por si solo (o ayudado por un agente impulsor, como el nitrógeno, añadido al propio agente extintor) o si el extintor portátil tiene un pequeño compartimiento, interno o externo, con un agente impulsor. Al primer tipo de extintores se les denomina de presión permanente, mientras que al segundo tipo de presión no permanente con botellín interior o exterior. Los de presión permanente se caracterizan por tener un manómetro que indica la presión del interior del extintor portátil.

Esquema 2.11

Los extintores portátiles deben contar con una inscripción que informe del tipo de agente extintor del que están provistos, para qué tipo o tipos de fuego es adecuado y modo de empleo, entre otros datos. Todo ello está especificado en el **Artículo 10 de la ITC-MIE-AP5**.

Deben estar situados en lugares donde haya más riesgo de sufrir un incendio, próximos a las salidas y siempre donde sean de fácil acceso y visibilidad, la parte superior del extintor portátil nunca deberá estar por encima de un metro y setenta centímetros. También cerca de donde haya elementos especialmente sensibles o críticos, como nuestros servidores de datos o *racks*. El agente extintor del que estén provistos deberá ser el adecuado para el fuego que se pudiera originar en el lugar donde se encuentre y su ubicación se ajustará a lo establecido en la Norma **UNE 23-110-75**.

Un factor a tener en cuenta con los extintores portátiles, es que su manejo debe ser preciso, puesto que la capacidad que tienen permite normalmente una única descarga de entre 10 y 40 segundos, que bien aplicada suele ser suficiente para apagar la mayoría de los incendios para los que están indicados. Por ello, es preciso que el personal de la entidad sepa como usarlos correctamente.

Como todos los elementos que componen nuestro sistema antiincendio, los extintores portátiles requieren un mantenimiento específico, el cual veremos más adelante.

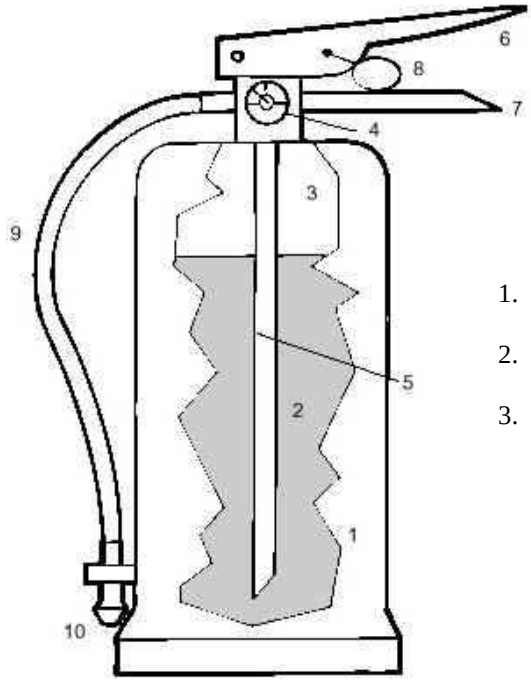
iii.i.ii) Bocas de incendio

Las bocas incendio son medios de extinción más potentes que los extintores portátiles, puesto que la cantidad de agente extintor que pueden aplicar es, como veremos a continuación, mucho mayor, sin embargo, el único agente extintor que pueden aplicar es el agua, por lo que solo se podrán emplear en fuegos del tipo A y en algunos casos del tipo B.

Esquema 2.11

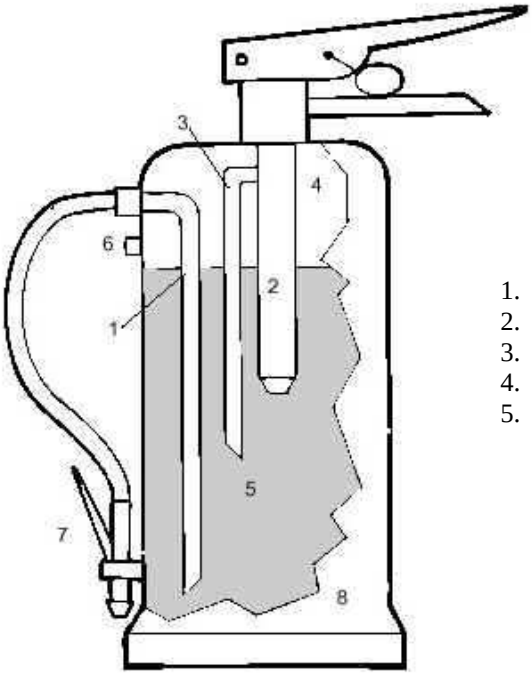
Tipos de extintores portátiles

a) Extintor portátil de presión permanente



1. Tubo de salida del agente extintor
2. Botellín de agente impulsor
3. Tubo de salida del agente impulsor
4. Cámara de gases
5. Agente extintor
6. Válvula de seguridad
7. Boquilla con palanca de accionamiento
8. Cuerpo del extintor

b) Extintor portátil de presión no permanente con botellín interior



1. Cuerpo del extintor
2. Agente extintor
3. Agente impulsor
4. Manómetro
5. Tubo sonda de salida
6. Maneta palanca de accionamiento
7. Maneta fija
8. Pasador de seguridad
9. Manguera
10. Boquilla de manguera

Este sistema está compuesto por los siguientes elementos: **boca de incendios equipada**, **red de tuberías de agua** y **fuente de abastecimiento del agua**. Vamos a ver cada elemento en profundidad.

iii.i.ii.i) Bocas de incendio equipadas (BIE)
Éstas podrán ser de dos tipos, de 25 o 45 milímetros y su ubicación en el edificio será sobre un soporte fijo, de tal manera que el centro quede a una distancia máxima de un metro y medio hasta el suelo. Deberán estar cerca de puertas y salidas, teniendo en cuenta que no deben constituir un obstáculo a la hora de usar dichas puertas. El número de bocas y su distribución será tal que permita cubrir por completo todas nuestras instalaciones, ya la distancia máxima entre bocas no debe exceder los 50 metros. Siempre se tiene que dejar una zona libre de obstáculos alrededor de éstas para poder accederlas fácil y rápidamente. Estarán equipadas a su vez por los siguientes elementos:

iii.i.ii.i.i) Una **boquilla** que permita la salida del agua en forma de chorro o pulverizada y que disponga de un sistema de cierre. Además el orificio de salida deberá estar dimensionado de forma que se consigan los caudales exigidos.

iii.i.ii.i.ii) Una **manguera** que podrá ser de 15 o 45 milímetros y que se ajustará a los establecido en las normas **UNE 23-091181**, **UNE 23-091182** y **UNE 23-091182**.

iii.i.ii.i.iii) Unos **racores** que unirán los distintos elementos. Todos han de estar solidamente unidos a estos elementos y han de cumplir la Norma **UNE 23-400181**.

iii.i.ii.i.iv) Una **válvula** que permita el cierre y la apertura del paso del agua y deberá estar realizada en material metálico resistente a la oxidación y corrosión. En el tipo de 25 milímetros, la válvula podrá ser de apertura automática al girar la devanadera.

iii.i.ii.i.v) Un **manómetro** que permita medir la presión que se alcanza. El rango del manómetro deberá ir desde cero hasta la presión máxima que puede alcanzar el sistema.

iii.i.ii.i.vi) Un **soporte** que deberá tener suficiente resistencia mecánica para soportar además del peso de la manguera las acciones derivadas de su funcionamiento. Se admite tanto el de tipo devanadera, carrete para conservar la manguera enrollada, como el de tipo plegadora, soporte para conservar la manguera doblada zigzag, excepto en el tipo de 25 milímetros, que será siempre de devanadera. Ambos tipos de soporte permitirán orientar correctamente la manguera. Para mangueras de 45 milímetros, el soporte deberá poder girar alrededor de un eje vertical.

iii.i.ii.i.vii) Para el tipo de mangueras de 45 milímetros es obligatorio, y recomendable para el de 25 milímetros, que todos los elementos estén recogidos en un **armario** de dimensiones suficientes para permitir un despliegue rápido y completo de la manguera. Éste podrá ser empotrado o de superficie, siendo en este caso metálico. En todos los casos la tapa será de marco metálico y provista de un cristal que posibilite la fácil visión y accesibilidad, así como la rotura del mismo. Dispondrá de un sistema que permita su apertura para las operaciones de mantenimiento. Su interior estará ventilado.

iii.i.ii.ii) Red de tuberías

La red de tuberías será de acero, pudiendo ser de otro material cuando vaya enterrada o convenientemente protegida. De uso exclusivo para instalaciones de protección contra incendios y deberá diseñarse de manera que queden garantizadas, en cualquiera de las bocas de incendio equipadas, las siguientes condiciones de funcionamiento.

iii.i.ii.ii.i) La **presión** dinámica en punta de lanza será como mínimo de 3,5 Kg./cm^2 y como máximo de 5 Kg./cm^2.

iii.i.ii.ii.ii) Los **caudales** mínimos serán de 1,6 litros/segundo para bocas de 25 milímetros, y 3,3 litros/segundo para bocas de 45 milímetros.

iii.i.ii.ii.iii) Estas condiciones de presión y caudal se deberán mantener durante una hora, bajo la hipótesis de funcionamiento simultáneo de las dos bocas hidráulicamente más desfavorables.

iii.i.ii.ii.iv) La red se protegerá contra la corrosión, las heladas y las acciones mecánicas, en los puntos que se considere preciso.

iii.i.ii.iii) Fuente de abastecimiento de agua

Normalmente, el abastecimiento de agua para estos sistemas de extinción provendrá de los servicios públicos de abastecimiento de agua, siempre que éstos garanticen las condiciones exigidas de presión y continuidad. La toma para será independiente de de cualquier otro uso y no podrá disponer ni de contadores ni de válvulas cerradas.

Si los servicios públicos de abastecimiento de agua no pudieran garantizar las condiciones de suministro establecidas en el anterior apartado, será necesario instalar en el edificio un depósito de agua con capacidad suficiente y equipos de bombeo adecuados para garantizar dichas condiciones. Estos equipos de bombeo serán de uso exclusivo para estos los sistemas antiincendio. Una alternativa a ésta es alimentar el sistema de bocas antiincendio desde una red general de incendios común a otras instalaciones de protección, siempre y cuando en el cálculo de abastecimiento se hayan tenido en cuenta los mínimos requeridos para cada una de las instalaciones que han de funcionar simultáneamente.

Estos sistemas, por ser exclusivamente para uso en fuegos de tipo A y en algunos casos en fuegos del tipo B, no serán adecuados para proteger nuestro centro computacional, ya que no debe emplearse este sistema en fuegos con peligro de electrocución. Además, como ya hemos comentado, el agua es perjudicial para los sistemas electrónicos.

iii.ii) Métodos automáticos

Los sistemas automáticos son aquellos que no necesitan la intervención de ningún individuo para ponerse en funcionamiento. Como ya hemos mencionado anteriormente, son fijos y actúan inundando por completo del agente extintor del que estén provistos su zona de actuación. Aunque estemos hablando de métodos automáticos, normalmente existe, y sobre todo en los que están instalados en los lugares más críticos, un pulsador para activarlos manualmente, de esta manera si un empleado detecta un incendio podrá activar el sistema de extinción con suma premura, incluso antes de que el sistema antiincendios lo detecte.

Al igual que los extintores portátiles, los sistemas automáticos se clasifican dependiendo del agente extintor que pueden aplicar, teniendo unas características determinadas.

En cualquier caso, los sistemas contarán con cuatro elementos básicos: **los rociadores**, que estarán colocados en el techo de tal manera que abarquen toda la zona a proteger. **Una válvula** que permita el paso del agente extintor cuando la alarma sea activada. **Una fuente de suministro** del agente extintor, que dependiendo de éste serán depósitos adecuados o, en el caso de que sea agua, podrá ser la fuente general del edificio y un **conjunto de cañerías**, por las que viaja el agente extintor desde la fuente de suministro hasta los rociadores.

Normalmente, los sistemas automáticos están **conectados a la unidad de control del sistema antiincendios**. Cuando nuestros detectores envían la señal de alarma, la central de control activa los extintores automáticos. Existe otro modelo, el cual es **independiente del sistema principal de alarma**. Disponen de una válvula en el propio rociador que al detectar calor permite el paso del agente extintor.

Aunque hemos comentado que los extintores automáticos aplican el agente extintor a toda la zona que compone su campo de acción, existen dos tipos de extintores, de **inundación total** y de **protección por objetivo**. Los de inundación total aplican el agente extintor de tal manera que el sector de incendio que protegen se llene de éste. Los extintores por objetivo aplican el agente extintor solamente a un elemento concreto, principalmente a los que son especialmente propensos o sufrir incendios, como un depósito de combustible o los que son críticos para la entidad, como servidores de datos Es por ello que los tendremos en cuenta a la hora de hablar de la protección en el centro computacional. Los rociadores de protección por objetivo serán únicamente los que empleen un agente extintor gaseoso, como veremos más adelante.

iii.ii.i) Sistemas rociadores de agua

Éstos emplean como agente extintor el agua y deben cumplir con las especificaciones expuestas en las normas **UNE 23-590-81**, **UNE 23-591-81**, **UNE 23-592-81**, **UNE 23-593-81** y **UNE 23-594-81** y se dispondrán de características y el número adecuados para cubrir por completo la zona que se desea proteger.

El abastecimiento de agua debe ser por tuberías independientes, y las características deben ser las mimas que para las bocas de incendio equipadas (BIE) ya visto. La instalación se someterá a una prueba de estanquidad y resistencia mecánica y a una presión hidrostática igual a la máxima presión de servicio más 3,5 Kg./cm^2 y con un mínimo de 14 Kg./cm^2, manteniendo dicha presión de prueba durante dos horas y no debiendo aparecer fugas en ningún punto de la instalación. La instalación se someterá, antes de su recepción, a las pruebas de control de funcionamiento establecidas.

En caso de que los equipos de bombeo sean eléctricos, deberán tener una redundancia en el suministro de energía, por alguno de los métodos que ya hemos visto.

iii.ii.ii) Sistemas rociadores de polvos químicos secos

Emplean como agente extintor los polvos polivalentes ABC o los polvos normales BC y su instalación se ajustará a lo establecido en las normas **UNE 23-541-79** y **UNE 23-543-79**. El polvo se almacena en unos depósitos que cumplirán con las normas establecidas, donde se debe indicar el tipo de agente extintor que contienen. Al enviar la unidad de control la señal de alarma, los rociadores permitirán el paso del agente extintor, rociando con éste el área de acción.

iii.ii.iii) Sistemas rociadores de agentes extintores gaseosos

Este tipo de sistemas emplean agentes extintores gaseosos, como pueden ser el CO_2, los gases halogenados o los gases inertes y, como ya hemos comentado, la instalación de estos dispositivos podrá ser de dos tipos, de inundación total y por objetivo. Los sistemas de inundación total se utilizarán para zonas amplias y sectores de incendio al completo, mientras que los sistemas por objetivo se emplearán para cubrir elementos o zonas muy concretas, quedando emplazados de tal manera que la descarga quede orientada hacia el elemento a proteger y que cubra toda la extensión del mismo.

Este tipo de sistemas deben contar con un sistema de retardo de disparo, es decir, que un avisador acústico y óptico notifique con el tiempo suficiente para desalojar la zona, que se va a aplicar el agente extintor. En caso de que el agente extintor sea nocivo para la salud, por su toxicidad o por dejar el nivel de oxígeno por debajo del 12%, deberá existir un pulsador en el área de acción del rociador que permita detener de manera inmediata la aplicación del agente extintor para que el personal que pudiera estar en esta zona salga de ésta de manera segura.

f) Adecuación de de agentes extintores a tipos de fuegos y sistemas de aplicación

Dado que existen un gran número de agentes extintores, cada uno ideado para un tipo de fuego concreto y varios sistemas para aplicarlo, vamos a ver un cuadro resumen que nos aclare qué agente extintor es adecuado para cada tipo de fuego y para qué medio de aplicación. Así como cuales son aplicables en presencia de gente, cuales permiten una buena visibilidad y cuales dejan residuos tras su aplicación. Queda detallado en el siguiente esquema.

Esquema 2.12

Esquema 2.12

Adecuación de de agentes extintores a tipos de fuegos y sistemas de aplicación

Siendo: - No adecuado • Aceptable •• Adecuado ••• Muy adecuado
Notas:
BV/AG/R – ¿Buena Visibilidad? / ¿Aplicable con Gente? / ¿Deja Residuos?
(1) Hasta tensión máxima indicada
(2) Sin sobrepasar el límite de concentración indicado

TIPO	AGENTE BV/AG/R	AUTOMÁTICO	POR OBJETIVO	A	B	C	D	CON RIESGO DE ELECTROCUCIÓN
			POR INUNDACIÓN	A	B	C	D	CON RIESGO DE ELECTROCUCIÓN
		MANUAL	EXTINTOR PORTÁTIL	A	B	C	D	CON RIESGO DE ELECTROCUCIÓN
			BOCA DE INCENDIO EQUIPADA	A	B	C	D	CON RIESGO DE ELECTROCUCIÓN
AGUA	PULVERIZADA SI/SI/SI	•••	-	-	-	-	-	-
			•••	•••	•	-	-	-
		•••	•••	•••	•	-	-	-
			•••	•••	•	-	-	-
	A CHORRO SI/SI/SI	-	-	-	-	-	-	-
			-	-	-	-	-	-
		•••	-	-	-	-	-	-
			•••	••	-	-	-	-
ESPUMA	ESPUMA SI/SI/SI	-	-	-	-	-	-	-
			-	-	-	-	-	-
		•••	•••	••	••	•	-	-
			-	-	-	-	-	-
POLVOS QUÍMICOS SECOS	NORMALES BC NO/SI/SI	••	-	-	-	-	-	-
			••	-	•••	••	-	•• (1)
		•••	•••	-	•••	••	-	•• (1)
			-	-	-	-	-	-
	POLIVALENTES ABC NO/SI/SI	••	-	-	-	-	-	-
			•••	•••	••	••	-	••• (1)
		•••	•••	•••	••	••	-	••• (1)
			-	-	-	-	-	-
GASES INERTES	CO_2 SI/SI(2)/NO	•••	-	-	-	-	-	-
			•••	••	••	•	-	•
		•••	•••	••	••	•	-	••
			-	-	-	-	-	-
	ARGÓN SI/SI(2)/NO	•••	-	-	-	-	-	-
			•••	••	••	••	-	••
		•••	-	-	-	-	-	-
			-	-	-	-	-	-
	50% ARGÓN + 50% NITRÓGENO SI/SI(2)/NO	•••	-	-	-	-	-	-
			•••	••	••	••	-	••
		-	-	-	-	-	-	-
			-	-	-	-	-	-

GASES HALOGE_ NADOS	**HFC-227ea SI/SI/NO**	•••	•••	••	•••	-	-	•••
			•••	••	•••	-	-	•••
		•••	•••	••	•••	-	-	•••
			-	-	-	-	-	-
	HFC-23 SI/SI/NO	•••	•••	••	•••	-	-	-
			•••	••	•••	-	-	•••
		-	-	-	-	-	-	-
			-	-	-	-	-	-
	HCFC-mezcla A SI/SI/NO	•••	•••	••	•••	-	-	•••
			•••	••	•••	-	-	•••
		-	-	-	-	-	-	-
			-	-	-	-	-	-
	FS 49 C2 SI/SI/NO	•••	•••	••	•••	-	-	•••
			•••	••	•••	-	-	•••
		-	-	-	-	-	-	-
			-	-	-	-	-	-
	HCFC-mezcla C SI/SI/NO	-	-	-	-	-	-	-
			-	-	-	-	-	-
		•••	•••	••	•••	•••	-	•••
			-	-	-	-	-	-

g) Mantenimiento de los sistemas antiincendio

Dado que los elementos que componen nuestro sistema antiincendio es posible que estén muchos años instalados sin que tengan que intervenir y puesto que es muy difícil, por no decir imposible, comprobar que los sistemas instalados funcionan correctamente bajo las condiciones que se dan en un incendio, es tan importante como elegir un sistema adecuado, el tener un buen programa de mantenimiento con las revisiones necesarias, además de la adecuada formación teórico-práctica del personal.

Independientemente de las revisiones periódicas reglamentarias que exponemos a continuación, los equipos de lucha contra el fuego deberían ser contemplados también en las revisiones periódicas de los lugares de trabajo a realizar por los responsables de las diferentes unidades, a fin de detectar posibles anomalías frecuentes (localización y/o acceso dificultoso, ausencia de equipo, ubicación incorrecta, etc.). De esta forma se pretende que tales equipos sean considerados como algo propio de cada unidad funcional y, por tanto, sean controlados en primera instancia por los responsables directos de las distintas unidades.

Las revisiones que se exponen a continuación deberán ser llevadas a cabo por personal especializado del fabricante, del instalador o de la empresa mantenedora autorizada de los sistemas a revisar.

i) Sistemas automáticos de detección y alarma de incendios

i.i) Cada tres meses
- Comprobación de funcionamiento de las instalaciones (con cada fuente de suministro).
- Sustitución de componentes defectuosos, como pilotos, fusibles, etc.
- Mantenimiento de acumuladores (limpieza de bornes, etc.).

- Observaciones
Estos sistemas se ajustarán a las Normas UNE 23007/ Partes 1, 2, 4, 5, 5 con 1ª modificación, 6, 7, 8, 9, 10 y 14. El mantenimiento detallado se ajustará a la Norma UNE 23007/14. Los detectores de incendio antes de su fabricación o importación han de ser aprobados de acuerdo al artículo 2° del Reglamento.

i.ii) Cada año
- Verificación integral de la instalación.
- Limpieza del equipo de centrales y accesorios.
- Verificación de uniones roscadas o soldadas.
- Limpieza y reglaje de relés.
- Regulación de tensiones e intensidades.
- Verificación de los equipos de transmisión de alarma.
- Prueba final de la instalación con cada fuente de suministro eléctrico.

ii) Sistema manual de alarma de incendios

ii.i) Cada tres meses
- Comprobación de funcionamiento de las instalaciones (con cada fuente de suministro).

- Mantenimiento de acumuladores (limpieza de bornes, etc.).

- Observaciones
Constituidos por: Conjunto de pulsadores. Central de control vigilada. Fuentes de alimentación, se regirán por Norma UNE 23007/Partes 1, 2 y 4. Distancia máxima a pulsadores desde cualquier punto 25 m.

ii.ii) Cada año
- Verificación integral de la instalación.
- Limpieza de sus componentes.
- Verificación de uniones roscadas o soldadas.
- Prueba final de la instalación con cada fuente de suministro eléctrico.

iii) Extintores portátiles de incendio

iii.i) Cada tres meses
- Comprobación de la accesibilidad, señalización, buen estado aparente de conservación.
- Inspección ocular de seguros, precintos, inscripciones, etc.
- Comprobación del peso y presión en su caso.
- Inspección ocular del estado externo de las partes mecánicas (boquilla, válvula, manguera, etc.).

- Observaciones
Se regirán por el Reglamento de Aparatos a Presión y su ITC MIE-AP5. Deberán ser aprobados según Art. 2° del Reglamento de instalaciones de protección contra incendios a efectos de justificar el cumplimiento de la Norma UNE 23110/ Partes 1, 2, 3, 4, 5 y 6. El mantenimiento con las pruebas periódicas está en la UNE 23120. Se ubicarán en lugares fácilmente visibles y accesibles. Deberán estar próximos a los puntos con riesgo de incendios y a las salidas y la parte superior como máximo a 1,70 m del suelo. Adecuación a clase de fuego según UNE EN 2-1992.

iii.ii) Cada año
- Comprobación del peso y presión en su caso.
- En el caso de extintores de polvo con botellín de gas de impulsión se comprobará el buen estado del agente extintor y el peso y aspecto externo del botellín.
- Inspección ocular del estado de la manguera, boquilla o lanza, válvulas y partes mecánicas.

- Observaciones
Los extintores deberán cumplir el Reglamento de Aparatos a Presión y su ITC MIE-AP5. Serán aprobados según el Art. 2° del Reglamento de instalaciones de protección contra incendios a efectos de justificar el cumplimiento de la Norma UNE 23010/1, 2, 3, 4, 5 y 6. Serán fácilmente visibles y accesibles. Estarán próximos a puntos con riesgo de incendios y a las salidas. Su instalación será preferentemente en paramentos verticales, con la parte superior, como máximo a 1,70 m del suelo.

iii.iii) Cada cinco años

A partir de la fecha de timbrado del extintor en su placa de diseño o etiqueta de pruebas de presión (y por tres veces) se retimbrará el extintor de acuerdo con la ITC-MIE AP5 del Reglamento de Aparatos a Presión sobre extintores de incendios (BOE 23.6.1982) y sus modificaciones por Orden 26.10.1983 (BOE 7.11.1983), Orden 31.5. 1985 (BOE 20.6.1985), Orden 15.11.1989 (BOE 28.11.1989) y Orden 10.3. 1998 (BOE 28.4.1998, rect. 5.6.1998). El detalle de las operaciones está indicado en la Norma UNE 23120 Mantenimiento de extintores portátiles contra incendios.

iv) Bocas de incendio equipadas (BIE)

iv.i) Cada tres meses
- Comprobación de la buena accesibilidad y señalización de los equipos.
- Comprobación por inspección de todos los componentes, procediendo a desenrollar la manguera en toda su extensión y accionamiento de la boquilla caso de ser de varias posiciones.
- Comprobación, por lectura del manómetro, de la presión de servicio.
- Limpieza del conjunto y engrase de cierres y bisagras en puertas del armario.

- Observaciones
Los sistemas de BIE constan de: Una fuente de abastecimiento de agua, con la red de tuberías y los armarios BIE necesarios. El centro de BIE de 45 milímetros y la boquilla de BIE de 25 milímetros deberán estar ubicadas a una altura máxima de 1,5 m del suelo y a una distancia máxima de 25 m de cualquier punto protegido. La separación máxima entre cada BIE y su más cercana 50 m. Se regirán por el Art. 2 del Reglamento de instalaciones de protección contra incendios y según las normas UNE EN 671/1 y 2. Pueden existir dos tipos: BIE de 45 y de 25 milímetros.

iv.ii) Cada año
- Desmontaje de la manguera y ensayo de ésta en lugar adecuado.
- Comprobación del correcto funcionamiento de la boquilla en sus distintas posiciones y del sistema de cierre.
- Comprobación de la estanquidad de los racores y manguera y estado de las juntas.
- Comprobación de la indicación del manómetro con otro de referencia acoplado en el racor de conexión de la manguera.

- Observaciones
Las BIE están constituidas por una fuente de abastecimiento de agua, la red de tuberías, y las BIE's necesarias. El centro deberá situarse como máximo a 1,5 m de altura y a ser posible a una distancia máxima de 5 m de las salidas. Separación máxima de 50 m entre dos BIE's, y no exceder 25 m de cualquier punto protegido. Deberán ser aprobadas según lo indicado en el Art. 2° del Reglamento de instalaciones de protección contra incendios y las Normas UNE-EN 671-1 y UNE-EN 671-2. Podrán ser de dos tamaños: BIE 45 milímetros y BIE 25 milímetros, según el nivel de riesgo.

iv.iii) Cada cinco años
- La manguera debe ser sometida a una presión de prueba de 15 Kg./cm2.

v) Sistemas automáticos y fijos de aplicación de agente extintor

v.i) Cada tres meses
- Comprobación de que las boquillas del agente extintor o rociadores están en buen estado y libres de obstáculos, para su funcionamiento correcto.
- Comprobación del buen estado de los componentes del sistema, especialmente de la válvula de prueba en los sistemas de rociadores, o los mandos manuales de la instalación de los sistemas de polvo, o agentes extintores gaseosos.
- Comprobación del estado de carga de la instalación de los sistemas de polvo, anhídrido carbónico, o hidrocarburos halogenados y de las botellas de gas impulsor cuando existan.
- Comprobación de los circuitos de señalización, pilotos, etc., en los sistemas con indicaciones de control.
- Limpieza general de todos los componentes.

- Observaciones
Los Rociadores Automáticos deberán regirse por: Normas UNE 23590 y 23595/ 1, 2 y 3. Los Sistemas de Extinción por Agua Pulverizada deberán regirse por: Normas UNE 23501 a 23507. Los Sistemas de Extinción por Espuma Física, se regirán por: Normas UNE 23521 a 23526. Los Sistemas de Extinción por Polvo seguirán: Normas UNE 23541 a 23544. Los Sistemas de Extinción por Agentes Gaseosos serán solo utilizables cuando quede garantizada la seguridad incluyendo la evacuación del personal. El mecanismo de disparo será por detectores de humo, elementos fusibles, termómetro de contacto o termostato o disparo manual en lugar accesible. Incluirá un retardo en su acción y un sistema de *prealarma*.

v.ii) Cada seis meses
- Comprobación de la accesibilidad de la entrada de la calle y tomas de piso.
- Comprobación de la señalización.
- Comprobación de las tapas y correcto funcionamiento de sus cierres (engrase si es necesario).
- Comprobar que las llaves de las conexiones siamesas están cerradas.
- Comprobar que las llaves de seccionamiento están abiertas.
- Comprobar que todas las tapas de racores están bien colocadas y ajustadas.

v.ii) Cada año
- Comprobación integral, de acuerdo con las instrucciones del fabricante o instalador, incluyendo en todo caso las siguientes revisiones:
- Verificación de los componentes del sistema, especialmente los dispositivos de disparo y alarma.
- Comprobación de la carga de agente extintor y del indicador de la misma (medida alternativa del peso o presión).
- Comprobación del estado del agente extintor.
- Prueba de la instalación en las condiciones de su recepción.

- Observaciones
Los rociadores automáticos de agua seguirán las Normas UNE 23590 y UNE 23595/1, 2 y 3. Los sistemas de extinción de agua pulverizada seguirán las Normas UNE 23501, UNE 23502, UNE 23503, UNE 23504, UNE 23505, UNE 23506 y UNE 23507. Los sistemas de extinción de espuma física de baja expansión se ajustarán a las Normas UNE 23521, UNE 23522, UNE 23523, UNE 23524, UNE 23525 y UNE 23526. Los

sistemas de extinción con polvo, deberán ajustarse a las Normas UNE-23541, UNE-23542, UNE-23543 y UNE-23544. Los sistemas de extinción con agentes gaseosos serán sólo utilizables cuando quede garantizada previamente la seguridad o la evacuación del personal. El mecanismo de disparo será accionado de forma automática o manual e incluirá un retardo en su acción y un sistema de prealarma.

vi) Abastecimiento de agua contra incendios

vi.i) Cada tres meses
- Verificación por inspección de todos los elementos, depósitos, válvulas, mandos, alarmas motobombas, accesorios, señales, etc.
- Comprobación de funcionamiento automático y manual de la instalación de acuerdo con las instrucciones del fabricante o instalador.
- Mantenimiento de acumuladores, limpieza de bornes (reposición de agua destilada, etc.).
- Verificación de niveles (combustible, agua, aceite, etc.).
- Verificación de accesibilidad a elementos, limpieza general, ventilación de salas de bombas, etc.

- Observaciones
El sistema de abastecimiento de agua contra incendios se ajustará a la Norma UNE 23500.

vi.ii) Cada seis meses
- Accionamiento y engrase de válvulas.
- Verificación y ajuste de prensaestopas.
- Verificación de velocidad de motores con diferentes cargas.
- Comprobación de alimentación eléctrica, líneas y protecciones.

vi.iii) Cada año
- Programa de mantenimiento anual de motores y bombas de acuerdo con las instrucciones del fabricante.
- Limpieza de filtros y elementos de retención de suciedad en la alimentación de agua.
- Prueba del estado de carga de baterías y electrolito de acuerdo con las instrucciones del fabricante.
- Prueba, en las condiciones de su recepción, con realización de curvas del abastecimiento con cada fuente de agua y de energía.

- Observaciones
El sistema de abastecimiento de agua contra incendios se ajustará a la Norma UNE 23500.

Para conseguir un buen control del plan de mantenimiento se puede recurrir al uso de unas fichas de datos sobre los medios materiales disponibles en las que consten la referencia del plano de ubicación, la zona, el código de la instalación o elemento controlado, sus características, la empresa responsable del mantenimiento, periodicidad mínima de revisión, fecha de la última revisión, fecha de caducidad (si procede) y observaciones. Estos datos pueden ser informatizados de manera que, al establecerse

una consulta mensual sistematizada, aparezca en el listado de ordenador la actualidad de cada elemento controlado, pudiendo saberse el número total de las revisiones a realizar en ese mes, así como las sustituciones precisas y las observaciones sobre el estado de conservación u otras incidencias.

Independientemente de las operaciones anuales y quinquenales reglamentadas a realizar por el fabricante, instalador del equipo o sistema o por una empresa mantenedora autorizada, están las otras **operaciones trimestrales y semestrales que pueden llevarse a cabo** por empresa mantenedora autorizada o **por el usuario de la instalación**.

Estas últimas en caso de realizarse por el propio usuario pueden distribuirse racionalmente entre el personal de producción y el de mantenimiento, asignando las comprobaciones que no necesiten desmontaje, calibración o medida a los operarios de producción del área, y las que sí lo requieran, al de mantenimiento. En algunas de estas últimas se puede implicar al grupo propio de lucha contra incendios, como por ejemplo las relativas a los extintores, en lo que se refiere a su accesibilidad, estado aparente de conservación, estado de carga del extintor y del botellín de gas impulsor así como el estado de las partes mecánicas.

2.4.3 - Inundaciones

Como ya hemos comentado, el agua es un gran enemigo de los sistemas eléctricos, por lo que éstos deberán estar lo más protegidos posible ante una inundación. Al igual que los incendios, las inundaciones pueden producirse tanto en el exterior como en el interior de nuestras instalaciones. Ya hemos mencionado cómo se pueden producir en el exterior y las medidas que tenemos que tomar al respecto, vamos a ver ahora de qué manera se pueden originar en el interior de nuestro edificio, cómo las podemos prevenir, detectar y cómo minimizar los daños que nos puedan causar.

Generalmente, las inundaciones en el interior de las instalaciones se pueden producir por dos motivos. El primero es por la **rotura de cañerías** o tuberías por las que se canaliza el agua de abastecimiento a nuestro edificio. Es una situación poco frecuente, pero muy a tener en cuenta. El segundo motivo por el cual se puede producir una inundación es que un **elemento que disponga de agua (bocas de agua)**, como grifos, baños, bocas de incendio, etc. se averíe o se obstruya el desagüe correspondiente.

La mejor manera de proteger nuestros sistemas más críticos ante una posible inundación es alejándolos de los elementos que la pudiera provocar, ya que normalmente las inundaciones que se producen en el interior del edificio afectan a una zona muy concreta. Para esto se debe actuar a la hora de distribuir nuestras instalaciones, puesto que no suele ser tarea fácil cambiar las tuberías o baños de emplazamiento, lo mejor será disponer nuestros sistemas críticos lejos éstos.

Para detectar cuando se ha producido un escape de agua, disponemos de unos **sensores de humedad**. Éstos son unos aparatitos muy pequeños que, colocados en el suelo, al detectar agua emiten una señal acústica. Normalmente funcionan con baterías y son totalmente independientes del sistema de alarma central, lo cual es un inconveniente si se produjera una inundación en nuestras instalaciones en un horario en el que no hay

nadie para poder subsanarla, por ejemplo, por la noche. Veremos a continuación cómo y donde debemos colocar estos detectores.

a) Cañerías

Todos los elementos que canalizan el agua por el interior de nuestro edificio, como puedan ser tuberías, cañerías o desagües pueden, en un momento dado, provocar una inundación. Como ya hemos mencionado, lo mejor es mantener los sistemas críticos lejos de las canalizaciones de agua, por lo que por nuestro centro computacional no deben pasar más que las necesarias para los sistemas antiincendio. En cualquier caso, las tuberías deben estar siempre por debajo del nivel en el que se encuentran nuestros sistemas eléctricos.

Las canalizaciones pueden estar al descubierto o empotradas en suelos y paredes, pero debemos saber exactamente por donde pasan todas y cada una de éstas, para de así conocer cuales son los puntos donde existe mayor riesgo de inundación.

En principio, el sistema de cañerías deberá ser manipulado únicamente por personal cualificado, pero se debe llevar un pequeño control para verificar que está todo en perfecto estado. Exceptuando las cañerías especificas de los sistemas antiincendio, que tienen una regulación especial, se debe controlar, por lo menos, una vez cada seis meses que ninguna cañería de fácil acceso tiene perdidas de agua. Entendemos por cañerías de fácil acceso todas aquellas que están a la vista o que podemos acceder a ellas fácilmente, como las que se encuentran entre el falso suelo y el piso real, ya que obviamente no vamos a levantar el suelo o a agujerear una pared para verificar que la cañería que pasa por su interior se encuentra en perfecto estado.

Los sensores de humedad se deben colocar cerca de las tuberías que se encuentren metidas en falsos suelos o poco visibles, puesto que si se produjera un escape por una de éstas, no nos percataríamos hasta que el agua subiera al nivel del falso suelo.

b) Bocas de agua

Como ya hemos mencionado, las bocas de agua son todos los elementos, al margen de las cañerías, que transfieren agua, como grifos, baños, etc. Al igual que ocurre con las cañerías, debemos alejar lo más posible nuestros sistemas más críticos de los lugares donde estén este tipo de elementos, como los baños, y procurar siempre que éstos estén bajo el nivel de nuestro centro computacional.

A excepción de los sistemas antiincendios que tienen unas revisiones y mantenimiento específico, estos elementos deben ser manipulados únicamente por personal cualificado, aunque debemos revisar periódicamente que ninguno tiene pérdidas de agua y que funcionan correctamente. Además, debemos verificar que los desagües correspondientes, así como los desagües cercanos, están limpios y operativos. Puesto que estos elementos suelen estar a la vista, si se produjera un escape de agua sería rápidamente percibido, no obstante, es conveniente colocar sensores de agua en lugares estratégicos que nos puedan indicar que se está produciendo un escape.

En cualquier caso, para estar protegidos ante una posible inundación, sea cual sea su origen, el edificio debe contar con paredes y techos protegidos, para evitar que el agua pueda circular rápidamente de un departamento a otro. Se deben disponer de drenajes entre los falsos suelos y el piso real. A excepción de los sistemas antiincendios, el suministro de agua del edificio debe contar con llaves de paso locales y una general, de tal manera que si se produjera un escape de agua de gran magnitud, se pueda cortar el suministro de agua y evitar una catástrofe mayor.

2.4.4 - Polvo

Como ya hemos mencionado, el polvo es un gran enemigo de los sistemas eléctricos y especialmente de los informáticos. Las partículas de polvo viajan a través del aire ambiental y terminan por depositarse en los objetos y superficies que se encuentra a su paso. Los PC´s, los *racks* o los servidores son, generalmente, elementos cerrados a través de los cuales circula una corriente de aire para su ventilación. Si el aire que atraviesa estos sistemas contiene partículas de polvo, éstas se van depositando en el interior, así como en los ventiladores y partes móviles, creando una película de polvo que dificulta enormemente la ventilación, haciendo, por tanto, que disminuya el rendimiento de estos sistemas. Además, existen cierto tipo de partículas de polvo que pueden llegar a ser conductores de la electricidad, por lo que podrían provocar un cortocircuito en nuestros sistemas eléctricos. Por otro lado, si el polvo se acumulara en la cabezas lectoras o elementos móviles de cualquier tipo de lector, podría dejarlo inoperante.

Como ya hemos visto, el polvo puede provenir del exterior de nuestras instalaciones, pero también puede generarse en el interior de éstas. Ya sabemos como actuar para hacer frente al polvo proveniente del exterior. Vamos a ver ahora como evitar que el polvo que se genera en el interior de nuestro edificio, por el uso diario de éste o por el desgaste de las fibras que componen los elementos, afecte a nuestros sistemas. Para prevenir en la medida de lo posible que se generen partículas de polvo en el interior del edificio, debemos disponer de mobiliario y elementos confeccionados con fibras que no generen polvo.

Es por ello que, aparte de disponer de filtros en las entradas de aire de nuestros sistemas de ventilación que retengan las partículas de polvo, debemos hacer que el aire del que disponemos en el interior de nuestras instalaciones pase por estos filtros periódicamente. Como veremos más adelante, para las zonas donde tengamos los equipos sensibles al polvo, como PC´s o *racks*, deberemos colocar además filtros adicionales. Estos filtros para retener las partículas de polvo requieren un mantenimiento, deben ser limpiados y/o sustituidos con la frecuencia que indique el fabricante, así como cada vez que creamos oportuno.

En cualquier caso, provenga el polvo del exterior o del interior de nuestras instalaciones, es necesario mantener una buena limpieza. Para ello, y puesto que el polvo puede una vez posado volver al aire para afectar a sistemas más delicados, se deben mantener los elementos superficiales, como suelos o mobiliario perfectamente libres de polvo. Se debe limpiar también con cierta asiduidad lugares menos accesibles, como falsos suelos o techos y bajo mesas y mobiliario en general.

2.5 - El entorno de los sistemas informáticos

Aunque podemos definir el entorno de los sistemas informáticos como todo lugar donde tengamos ubicado algún sistema informático, vamos a entender que es una sala especialmente equipada donde se albergan los sistemas más sensibles y críticos de que se disponen, además de los sistemas que tienen un alcance global a nivel de la entidad, como pueden ser servidores de datos, *racks*, terminales de administración o elementos hardware de red, entre otros.

Por tanto, debemos hacer una diferenciación entre equipos críticos, como servidores, elementos de red y equipos departamentales y las máquinas de usuario final. Por la importancia de los elementos críticos deben estar controlados y especialmente protegidos, y para ello lo mejor es tenerlos centralizados en lo que hemos venido llamando hasta ahora **centro computacional**. Se debe entender que es en esta sala donde vamos a desempeñar el mayor esfuerzo en lo que a Seguridad Física se refiere.

En cuando a las máquinas de usuario final, por lo general, las políticas de seguridad de cualquier entidad implican que no se tengan datos importantes almacenados en éstas, ya que estas máquinas son las más difíciles de proteger, por encontrarse en el entorno del usuario, descentralizado y de fácil acceso. Es importante que las pérdidas que pudieran suponer estas máquinas sean únicamente su valor económico.

En general, por la naturaleza de las medidas de Seguridad Física que vamos a comentar a continuación, se deberán aplicar, en mayor o menor medida, en todos los lugares donde tengamos elementos hardware o sistemas de información crítica para la entidad. En entidades no muy grandes, donde los sistemas de información compartan espacio con otro tipo de sistemas, se deberán aplicar medidas de Seguridad Física que cumplan con los requisitos de Seguridad de todos los elementos dispuestos, haciendo un mayor esfuerzo para proteger los elementos más críticos para la entidad.

Vamos a ver, por tanto, las posibles amenazas y situaciones que pueden poner en riesgo nuestro centro computacional y las estrategias que tenemos que adoptar para paliar sus efectos. En general, vamos a ver a un nivel más concreto y cercano al hardware lo que hemos venido viendo para el edificio en general.

2.5.1 - Los accesos físicos al centro computacional

En el centro computacional se deberá llevar un control total en todo momento de quién entra. Para ello es conveniente que el centro cuente con **una única entrada** en servicio y que ésta esté en todo momento cerrada, permitiendo el acceso únicamente a quien se valide, de una forma u otra. Siendo necesario además que la única manera de acceder físicamente a nuestro centro computacional sea a través de esta entrada.

a) El perímetro del centro computacional

Para lograr lo comentado anteriormente, el centro de cómputo deberá estar delimitado por paredes, suelo y techos consistentes, es decir, no podemos delimitar nuestro centro computacional con paredes móviles, mamparas o falsos suelos. Si existen estradas ocultas, tales como conductos de ventilación o desagües, deben tener una configuración tal, que impida el acceso físico al centro. En caso de que esto no sea así, o para mejorar la seguridad en caso de duda, se deben emplear en dichas entradas sensores que detecten una posible intrusión. Vamos a ver estos aspectos más detenidamente.

i) Paredes, suelos y techos deben ser fijos y consistentes. A ser posible deben ser de obra y es importante que no se puedan mover, derribar o perforar. En el caso de que encontremos un punto débil en alguno de los muros que delimitan nuestro centro de cómputo, deberemos emplear mecanismos que impidan el paso, así como sensores para detectar una posible intrusión. Dado que es habitual el uso de falsos suelos y techos, debemos cerciorarnos de que las paredes que delimitan el centro llegan hasta el piso real y no se quedan en el falso suelo o techo.

ii) En el caso de que existan ventanas, deberán disponer de detectores perimetrales y el centro debe contar con detectores de rotura de vidrios conectados a la unidad de control de nuestro sistema de alarma.

iii) Todas las posibles entradas ocultas, como desagües, falsos suelos o techos o conductos de ventilación por los que sea posible el acceso físico, deberán contar con sensores que detecten una posible intrusión. Estos detectores podrán ser cualquiera de los tipos que hemos visto anteriormente, aunque los más usuales son las barreras infrarrojas y los detectores espaciales.

iv) Como medida excepcional, podríamos intentar que todo el perímetro de nuestro centro de cómputo esté custodiado por cámaras de vigilancia, de tal manera que sea imposible acceder a éste sin ser detectado.

b) El acceso al centro computacional

Como ya hemos mencionado, nuestro centro computacional debe contar únicamente con una entrada en servicio, de tal manera que solo se pueda acceder al centro a través de ésta. La puerta de acceso debe estar siempre cerrada, de tal manera que permita la entrada o salida solo cuando la persona que accede se haya validado. Es importante que cada acceso al centro computacional quede reflejado, ya sea en un simple libro donde se vayan apuntando las personas que acceden o en un sistema automático que recoja la hora y el empleado que ha accedido al centro y lo guarde en un sistema electrónico de registros.

i) Validación

Para validarse en la entrada del centro computacional se debe emplear una de las técnicas que hemos visto anteriormente, algo que se sabe, algo que se tiene o algo que se es. Sin embargo, las técnicas para acceder al centro computacional deben ser más fuertes que las que se emplean para acceder al edificio, aunque no deben descuidar la cualidad de ser lo más cómodas y sencillas para quienes las tienen que usar a diario,

puesto que si suponen una molestia, se incentivaría el que se busquen métodos para evitar los mecanismos de seguridad.

i.i) Algo que se sabe
Como ya hemos visto, lo más normal es una contraseña que solamente conoce el personal autorizado para acceder al centro computacional. Es una técnica muy empleada, ya que colocando un pequeño teclado numérico en la puerta para introducir la clave de acceso, podemos garantizar una buena seguridad. Si existe una clave personal para cada miembro que tenga acceso, podemos realizar con este sistema un registro automatizado de entradas al centro. Es necesario que se siga una buena política de gestión y seguridad de contraseñas. Se puede emplear solo, pero es el complemento más empleado en sistemas mixtos, los cuales veremos más adelante.

i.ii) Algo que se tiene
Otro recurso muy empleado, ya que si no disponemos de un sistema de registro automatizado, simplemente una cerradura de seguridad con una llave convencional puede servir. También se pueden emplear tarjetas magnéticas para permitir el acceso. Esto es muy común, ya que la propia tarjeta de empleado la podremos emplear para acceder al edificio y a las zonas reservadas a las que cada uno estemos autorizados. Además permite el registro automatizado de accesos, puesto que las tarjetas deben ser personales e intransferibles.

i.iii) Algo que se es
El sistema de validación analiza factores inherentes a cada individuo. Estos sistemas de validación se denominan sistemas biométricos. Como hemos mencionado anteriormente, estos sistemas no se suelen implantar en las entradas generales al edificio, pero sí en los accesos a las zonas más restringidas, como puede ser nuestro centro computacional. Se puede realizar un análisis biométrico de cualquier característica inherente al individuo, pero los más comunes son **análisis de voz**, **de patrones oculares**, **de huella digital** y **de la geometría de la palma de la mano**. Podemos incluir además en este grupo la **firma escrita**, puesto que corresponde a un movimiento o acto involuntario (una persona al rubricar su firma no piensa en cada trazado individualmente).

Especialmente para este tipo de sistemas de validación debemos hablar de dos factores, la **tasa de falso rechazo** y la **tasa de falsa aceptación**. Por tasa de falso rechazo (*False Rejection Rate*, **FRR**) se entiende la probabilidad de que el sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente, y por tasa de falsa aceptación (*False Acceptance Rate*, **FAR**) la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo. Evidentemente, una FRR alta provoca descontento entre los usuarios del sistema, pero una FAR elevada genera un grave problema de seguridad ya que estamos proporcionando acceso a un recurso a personal no autorizado a acceder a él.

Estas dos tasas vienen definidas por cada sistema de autenticación, pero normalmente tienen un margen para modificarlas. Por ejemplo, en un sistema que analice la huella digital, si le configuramos para que mida 100 puntos tendrá una FRR y una FAR bajas, no rechazará a ningún usuario autorizado, pero un intruso podrá ser aceptado. Sin embargo si está configurada para que mida 10000 puntos tendrá una FRR y una FAR altas. Por lo que se debe tener en cuenta que estas dos tasas son proporcionales, es decir,

cuanto más alta sea la FAR menos posibilidades tendrá un intruso de ser aceptado por el sistema, pero además será también más elevada la FRR, la probabilidad de rechazar a un empleado autorizado.

El sistema óptimo sería aquel que tiene una FRR igual a cero y una FAR igual a uno, como es el caso de los sistemas de clave o llave, el que tiene la llave o conoce la clave es validado. Pero a estos sistemas hay que añadir el problema de pérdida, robo u olvido de los elementos de validación, lo cual es imposible con los sistemas biométricos.

Antes de ver los distintos sistemas biométricos de los que hemos hablado antes, conviene desmentir el mito de vulnerabilidad de estos sistemas a ataques de simulación. En cualquier película o libro de espías que se precie, siempre se consigue "engañar" a los sistemas biométricos para conseguir acceso a determinadas instalaciones mediante estos ataques. Se simula la parte del cuerpo a analizar mediante un modelo o incluso utilizando órganos amputados a un cadáver o al propio usuario vivo. Evidentemente, esto sólo sucede en la ficción, ya que hoy en día cualquier sistema biométrico, excepto quizá algún sistema de reconocimiento de voz, son altamente inmunes a estos ataques. Los analizadores de retina, de iris, de huellas o de la geometría de la mano son capaces, aparte de decidir si el miembro pertenece al usuario legítimo, de determinar si éste está vivo o se trata de un cadáver.

i.iii.i) Análisis de voz

Los sistemas de análisis o reconocimiento de voz no validan a los usuarios por lo que dicen, como mucha gente piensa, si no por cómo lo dicen. Cada persona tiene un determinado timbre y tono de voz, una forma determinada de pronunciar las sílabas, los hiatos o los diptongos, así como una velocidad determinada en la pronunciación, entre otras características de la voz.

Existen dos tipos de analizadores de voz, **de texto dependiente** y **de texto independiente**. Los de texto dependiente tienen guardada en la base de datos del sistema unas frases determinadas, por ejemplo, el nombre del usuario. Éste para validarse pronuncia la frase y el sistema, tras compararlas con las que tiene guardadas, autoriza o deniega el acceso. Como veremos a continuación, este sistema es mucho menos seguro que el de texto independiente. En este sistema, el analizador de voz propone una frase al usuario y éste la pronuncia para su validación.

El principal problema del reconocimiento de voz es la inmunidad frente a los *replay attacks*, un medio de ataque de simulación el cual consiste en que el atacante graba, por ejemplo, en un magnetófono, al usuario diciendo las frases o palabras que pronuncia para validarse en el sistema. Este problema es especialmente grabe en los sistemas de texto dependiente, ya que volviendo al ejemplo anterior, el del nombre de cada usuario, bastaría que un intruso grabara al usuario pronunciar su nombre para validarse en el sistema, por lo que en este tipo de sistemas de reconocimiento de voz se debe emplear junto con otro sistema de validación.

Este problema se solventa casi por completo en los sistemas de texto independiente, ya que el sistema propone al usuario una frase al azar para que la pronuncie, por lo que sería casi imposible que un intruso tuviera almacenadas en un dispositivo todas las palabras posibles pronunciadas por el usuario.

Sin embargo, el mayor problema de los sistemas de reconocimiento de voz consiste en que es posible que los usuarios tengan que repetir varias veces la frase para validarse. Esto es así porque existen muchos factores, como una pequeña congestión nasal o el estado de ánimo, que pueden variar el timbre de la voz. Otro factor que puede hacer que no se reconozca al usuario es el ruido que pueda haber en el ambiente a la hora de pronunciar la frase para validarse. Por tanto, estos sistemas se deben emplear en lugares donde no haya ruido ambiental. A su favor estos sistemas cuentan con una gran aceptación por parte de los usuarios, siempre y cuando no tengan que repetir varias veces las frases para ser validados.

i.iii.ii) Análisis de patrones oculares

Los modelos de autenticación biométrica basados en patrones oculares se dividen en dos tecnologías diferentes, **analizadores de retina** y **analizadores del iris**. Estos métodos se suelen considerar los más efectivos ya que para una población de 200 millones de potenciales usuarios la probabilidad de coincidencia es casi nula. Además una vez muerto el individuo los tejidos oculares degeneran rápidamente, lo que dificulta la falsa aceptación de atacantes que puedan robar este órgano de un cadáver. Aunque las dos tecnologías son muy similares, los analizadores de iris son más modernos y es el sistema biométrico más seguro.

La principal desventaja de los métodos basados en el análisis de patrones oculares es su escasa aceptación ya que el hecho de mirar a través de un binocular o monocular, necesario en ambas tecnologías, no es cómodo para los usuarios, ni aceptable para muchos de ellos dado que por un lado, los usuarios no se fían de un haz de rayos analizando su ojo, y por otro un examen de este órgano puede revelar enfermedades o características médicas que a muchas personas les puede interesar mantener en secreto, como el consumo de alcohol o de ciertas drogas.

Aunque los fabricantes de dispositivos lectores aseguran que sólo se analiza el ojo para obtener patrones relacionados con la autenticación, y en ningún caso se viola la privacidad de los usuarios, mucha gente no cree esta postura oficial. Aparte del hecho de que la información es procesada vía software, lo que facilita introducir modificaciones sobre lo que nos han vendido para que un lector realice otras tareas de forma enmascarada.

Por si esto fuera poco, se trata de sistemas demasiado caros para la mayoría de organizaciones, y el proceso de autenticación no es todo lo rápido que debiera en poblaciones de usuarios elevadas. De esta forma, su uso se ve reducido casi sólo a la identificación en sistemas de muy alta seguridad, como el control de acceso a instalaciones militares.

i.iii.iii) Análisis de la huella digital

Típicamente la huella digital o dactilar de un individuo ha sido un patrón bastante bueno para determinar su identidad de forma inequívoca, ya que está aceptado que dos dedos nunca poseen huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona. Así, desde el siglo pasado hasta nuestros días se vienen realizando con éxito clasificaciones sistemáticas de huellas dactilares en entornos policiales, y el uso de estos

patrones fue uno de los primeros en establecerse como modelo de autenticación biométrica.

Cuando un usuario desea autenticarse ante el sistema sitúa su dedo en un área determinada, área de lectura, no se necesita en ningún momento una impresión en tinta. Aquí se toma una imagen que posteriormente se normaliza mediante un sistema de finos espejos para corregir ángulos, y es de esta imagen normalizada de la que el sistema extrae las minucias que son ciertos arcos, bucles o remolinos de la huella, que va a comparar contra las que tiene en su base de datos. Es importante resaltar que lo que el sistema es capaz de analizar no es la huella en sí, sino que son estas minucias, concretamente la posición relativa de cada una de ellas. Está demostrado que dos dedos nunca pueden poseer más de ocho minucias comunes, y cada uno tiene al menos 30 o 40 de éstas.

Los sistemas basados en reconocimiento de huellas son relativamente baratos, en comparación con otros biométricos. Sin embargo, tienen en su contra la incapacidad temporal de autenticar usuarios que se hayan podido herir en el dedo a reconocer, ya que un pequeño corte o una quemadura que afecte a varias minucias pueden hacer inútil al sistema. También elementos como la suciedad del dedo, la presión ejercida sobre el lector o el estado de la piel pueden ocasionar lecturas erróneas. Otro factor a tener muy en cuenta contra estos sistemas es psicológico, como ya hemos dicho, un sistema de autenticación de usuarios ha de ser aceptable por los mismos, y generalmente el reconocimiento de huellas se asocia a los criminales, por lo que muchos usuarios recelan del reconocedor y de su uso, aunque no por ello deja de ser el sistema más usual y recomendado para proteger los centros que tratamos en este trabajo.

i.iii.iv) Análisis de la geometría de la palma de la mano

Los sistemas de autenticación basados en el análisis de la geometría de la mano son sin duda los más rápidos dentro de los biométricos: con una probabilidad de error aceptable en la mayoría de ocasiones, en aproximadamente un segundo son capaces de determinar si una persona es quien dice ser.

Cuando un usuario necesita ser autenticado sitúa su mano sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura. Una vez la mano está correctamente situada, unas cámaras toman una imagen superior y otra lateral, de las que se extraen ciertos datos (anchura, longitud, área, determinadas distancias, etc.) en un formato de tres dimensiones. Transformando estos datos en un modelo matemático que se contrasta contra una base de patrones, el sistema es capaz de permitir o denegar acceso a cada usuario.

Quizás uno de los elementos más importantes del reconocimiento mediante analizadores de geometría de la mano es que éstos son capaces de aprender ya que a la vez que autentican a un usuario, actualizan su base de datos con los pequeños cambios que se puedan producir en la muestra como un pequeño crecimiento, adelgazamiento, el proceso de cicatrizado de una herida, etc. de esta forma son capaces de identificar correctamente a un usuario cuya muestra se tomó hace años, pero que ha ido accediendo al sistema con regularidad. Este hecho, junto a su rapidez y su buena aceptación entre los usuarios, hace que los sistemas de validación basados en la geometría de la mano, junto con los de huella digital, sean los más extendidos dentro de los biométricos a

pesar de que su tasa de falsa aceptación se podría considerar inaceptable en algunas situaciones ya que no es normal, pero sí posible, que dos personas tengan la mano lo suficientemente parecida como para que el sistema las confunda. Para minimizar este problema se recurre a la identificación basada en la geometría de uno o dos dedos, que además puede usar dispositivos lectores más baratos y proporciona incluso más rapidez.

i.iii.iv) Análisis de firma escrita

Aunque la firma no es una característica estrictamente biométrica, como hemos comentado anteriormente se suele agrupar dentro de esta categoría ya que de la misma forma que sucedía en la verificación de la voz, el objetivo aquí no es interpretar o entender lo que el usuario escribe en el lector, sino autenticarlo basándose en ciertos rasgos tanto de la firma como de su rúbrica.

La verificación en base a firmas es algo que todos utilizamos y aceptamos día a día en documentos o cheques. No obstante, existe una diferencia fundamental entre el uso de las firmas que hacemos en nuestra vida cotidiana y los sistemas biométricos. Mientras que habitualmente la verificación de la firma consiste en un simple análisis visual sobre una impresión en papel, estática, en los sistemas automáticos no es posible autenticar usuarios en base a la representación de los trazos de su firma. En los modelos biométricos se utiliza además la forma de firmar, las características dinámicas (por eso se les suele denominar *Dynamic Signature Verification*, DSV) como el tiempo utilizado para rubricar, las veces que se separa el bolígrafo del papel, el ángulo con que se realiza cada trazo, la presión ejercida, etc.

Para utilizar un sistema de autenticación basado en firmas se solicita en primer lugar a los futuros usuarios un número determinado de firmas ejemplo, de las cuales el sistema extrae y almacena ciertas características; esta etapa se denomina de aprendizaje, y el principal obstáculo a su correcta ejecución son los usuarios que no suelen firmar uniformemente. Contra este problema la única solución, aparte de una concienciación de tales usuarios, es relajar las restricciones del sistema a la hora de aprender firmas, con lo que se disminuye su seguridad. Una vez que el sistema conoce las firmas de sus usuarios, cuando estos desean acceder a él se les solicita tal firma, con un número limitado de intentos, generalmente más que los sistemas que autentican mediante contraseñas, ya que la firma puede variar en un individuo por múltiples factores.

Podemos asegurar que **los sistemas biométricos en general** se acabarán imponiendo al resto, puesto que no es necesario que los usuarios recuerden contraseñas o claves y no cabe la posibilidad de que se olviden o extravíen tarjetas o llaves. El motivo por el cual no están implantados en la mayoría de las entidades hoy en día es porque es una tecnología reciente y aún con un precio más elevado que los métodos de autenticación clásicos.

c) Vigilancia del centro computacional

Por ser una zona especialmente sensible de nuestra organización, el centro computacional deberá disponer de una vigilancia especial. Para ello diferenciamos entre horas de oficina y cuando el centro está cerrado. Algunas medidas se deben aplicar sólo

cuando el centro está cerrado, otras cuando nuestros trabajadores están trabajando en él y otras se aplicarán en ambos casos.

i) Cuando el centro está cerrado
Cuando el centro esté cerrado debemos detectar la presencia de cualquier intruso que pueda estar en el interior de éste, por lo que debemos emplear detectores espaciales en el interior del centro computacional, de tal manera que el campo de acción de éstos cubra por completo el área del centro computacional. Debemos emplear también barreras infrarrojas que, colocadas en puntos estratégicos, detecten el paso de cualquier intruso. Los sensores que hemos comentado que deben estar presentes en el perímetro del centro computacional, deberán estar especialmente activos en las horas en las que éste se encuentre cerrado.

El uso de cámaras de vigilancia en estos centros puede ser un arma de doble filo, ya que si bien es un sistema para controlar lo que sucede en el interior de los centros de cómputo, puede que capten imágenes de elementos secretos de las entidades o acciones como la introducción de contraseñas en los PC´s por parte de los administradores, por lo que hay que tener sumo cuidado con el campo de acción de las cámaras.

ii) Cuando el centro está abierto
Cuando el centro está abierto debemos hacer hincapié en los sistemas de validación de acceso de los usuarios, puesto que en centros en los que haya mucho trasiego de personal puede que un intruso acceda al centro camuflado entre los trabajadores. Las cámaras de vigilancia deberán estar operativas también cuando nuestros empleados estén trabajando en el centro computacional, ya que pueden captar irregularidades anomalías en el uso de los elementos de éste. También pueden captar intrusos que han accedido de manera ilícita o posibles deficiencias en sistemas de seguridad, como puertas o ventanas abiertas.

2.5.2 - Suministro de energía eléctrica al centro computacional

Después de haber estudiado el suministro de energía al edificio debemos realizar un estudio del suministro de energía a los centros de computación o en el entorno inmediato donde se encuentra situado nuestro hardware. Como ya hemos mencionado, estos dispositivos necesitarán algún sistema de redundancia eléctrica para evitar posibles contratiempos originados por el corte de suministro eléctrico principal. Vamos a ver los factores más importantes a tener en cuenta, tanto en el sistema principal como en el auxiliar.

i) Potencia

Puesto que en el centro computacional dispondremos de una gran cantidad de aparatos eléctricos y algunos de ellos, como los sistemas de refrigeración, necesitan una gran potencia para funcionar, es necesario que la potencia de la línea eléctrica sea suficiente. Esto no suele ser un problema, puesto que como hemos comentado, la línea eléctrica suele estar sobredimensionada.

ii) Distribución

Dado que vamos a mantener un gran número de sistemas eléctricos en nuestro centro computacional, se deben colocar un gran número de enchufes y correctamente distribuidos, de tal manera que no sea necesaria la inclusión de alargadores o ladrones, que pueden llegar a ser muy peligrosos e inseguros. Previniendo el posible aumento de dispositivos en nuestro centro computacional, es necesario que exista un número mayor de tomas de corriente de las que en un principio podamos necesitar.

iii) Cableado

Los cables que abastecen de electricidad a nuestro centro computacional suelen estar empotrados en paredes y falsos suelos, y nunca deben estar a la vista ni por la superficie. Es importante que estén perfectamente aislados, para que de esta manera no puedan sufrir daños en caso de humedad o inundación. Además es importante que estén aislados de tal manera que no liberen energía electromagnética, que puede influir negativamente en nuestros sistemas.

iv) Ruido eléctrico

El ruido eléctrico es una alteración de la corriente eléctrica, producida generalmente por aparatos de gran consumo o motores. Esta alteración eléctrica, que pueden ser subidas o bajadas de tensión, variaciones en el voltaje, etc. se transmiten por los cables de corriente, llegando finalmente hasta los equipos o dispositivos conectados a estos. El ruido eléctrico puede llegar a dañar los sistemas, por lo que es necesaria la instalación de filtros en el circuito eléctrico en el que estén conectados nuestros sistemas críticos. Como ya hemos vistos, los SAI´s, especialmente los de nivel 5 y 9, incorporan este tipo de filtros.

v) Redundancia eléctrica

Hemos comentado ya que todos los sistemas críticos para la entidad, y en general, todos los sistemas de que disponemos en el centro computacional lo son, deben disponer de un sistema auxiliar de abastecimiento de energía eléctrica que permita, por lo menos, salvar todos los datos que se estaban manejando y apagar estos sistemas con seguridad, en caso de que la fuente principal de alimentación eléctrica falle.

Por lo tanto se debe emplear uno de los sistemas de redundancia eléctrica que ya hemos comentado. Hay que tener en cuenta siempre que no solo es necesario proveer de un suministro estable y continuo de energía a los ordenadores y a los sistemas de almacenamiento, deberemos proporcionar el mismo tratamiento al hardware de red y todos los dispositivos que sean necesarios para el funcionamiento normal de estos dispositivos críticos, como puede ser el sistema de ventilación, por lo que deberán estar dimensionados para ello.

Un buen sistema de distribución de la energía proveniente de los sistemas de redundancia consiste en que dispongamos de dos tipos de enchufes, diferenciados, por ejemplo, por su color. Un tipo dispondrán la energía proveniente únicamente del sistema de alimentación principal y el otro, además, suministrarán la energía de los sistemas de redundancia en caso de que el sistema principal falle. De ser así, es muy importante que en éstas tomas estén conectados únicamente los sistemas críticos, ya que si enchufáramos en éstas dispositivos secundarios, como una lámpara o el cargador de algún dispositivo portátil, estaríamos aumentando el consumo en el sistema auxiliar, reduciendo, por tanto, su tiempo de acción.

2.5.3 - El fuego en el centro computacional

Como ya hemos visto anteriormente, el fuego es posiblemente el factor más destructivo que nos podemos encontrar. Es por ello que nuestro centro computacional debe estar perfectamente protegido y contar con unas medidas especiales contra el fugo, además de las de ámbito general para todo el edificio. Algo importante a tener en cuenta es que el incendio se puede producir tanto en el interior como en el exterior del centro computacional.

Vamos a ver, al igual que hemos hecho con el interior del edificio, cómo prevenir, detectar, controlar y extinguir un incendio en el centro computacional, así como otros factores a tener en cuenta.

a) Tipo de fuego en el centro computacional

Lo primero que debemos conocer es el tipo de incendio que se producirá en el centro computacional, para así actuar de la manera más adecuada. Siguiendo la clasificación vista anteriormente, por la naturaleza de los dispositivos de que disponemos en el centro computacional, el fuego se alimentará de elementos sólidos, por lo tanto, **tipo A** y, obviamente, con alto **riesgo de electrocución**.

En el centro de cómputo no debemos tener almacenados bajo ninguna circunstancia ni líquidos ni gases inflamables que pudieran dar origen a un fuego de otro tipo, mucho más violento.

b) Prevenir un incendio en el centro computacional

Como ya hemos visto, existen tres elementos para que el fuego pueda iniciarse, por lo que si eliminamos uno de éstos no podrá comenzar un incendio. Los tres elementos son el oxígeno, la fuente de ignición y el combustible. Vamos a ver cada uno de ellos.

i) El oxígeno
Como ya hemos visto, es imposible eliminar el oxígeno de una zona como medida preventiva, ya que éste es necesario para llevar a cabo cualquier actividad.

ii) La fuente de ignición
Hemos cuales son las fuentes de ignición que pueden provocar un incendio. Para el caso del centro computacional, sólo cabe decir que se debe ser más restrictivo que en el resto del edificio. Vamos a ver qué medidas especiales se deben tomar.

ii.i) Llamas
Se debe prohibir terminantemente fumar, así como encender cualquier tipo de llama en el centro sin causa justificada.

ii.ii) Instalaciones y aparatos eléctricos
Dado que la práctica totalidad de los dispositivos que tenemos en nuestro centro computacional son eléctricos, la fuente de ignición más probable será un fallo eléctrico o cortocircuito. Por ello se debe verificar periódicamente que las instalaciones eléctricas se encuentran en perfecto estado y, ante cualquier anomalía, debe ser personal cualificado únicamente el que manipule las instalaciones o dispositivos averiados.

ii.iii) Fuentes de calor
Como veremos más adelante, es necesario que nuestros sistemas electrónicos se encuentren a una temperatura adecuada para funcionar correctamente. Es por ello que el centro debe contar con un sistema de climatización adecuado, por lo que deben estar prohibidas las estufas y demás elementos de esta índole, ya que pueden ser, además, la causa de un incendio.

iii) El combustible
En este aspecto, debemos tomar las mismas medidas que en el resto del edificio, pero como ya hemos mencionado, siendo más restrictivos. Vamos a comentar a grandes rasgos los aspectos generales a tener en cuenta.

iii.i) Techos y suelos
Es importante que los techos, suelos y paredes de nuestro centro de cómputo sean especialmente resistentes al fuego, ya sea por los materiales con los que están fabricados o por haberles aplicado elementos ignífugos.

iii.ii) El mobiliario
El mobiliario de nuestro centro computacional debe ser en su totalidad ignífugo. Elementos como sillas, mesas o armarios deben estar fabricados con material no inflamable para evitar que un posible incendio se propague rápidamente. Como veremos más adelante, los armarios de nuestro centro de cómputo deben ser armarios ignífugos, de esta manera los elementos y materiales que guardemos en éstos se encontrarán protegidos y evitaremos que se prendan, evitando por tanto que el incendio se propague.

iii.iii) Otros factores
Anteriormente hemos hablado de factores como elementos inflamables o la limpieza del interior de nuestras instalaciones. En el centro computacional debemos dar un paso más.

La limpieza de nuestro centro computacional debe ser total, todos los desperdicios deberán depositarse en los lugares adecuados. Las papeleras deberán vaciarse diariamente y deberán ser ignífugas. La zona que existe entre el falso suelo y el piso real deberá limpiarse con más asiduidad que en el resto del edificio.

No debemos almacenar elementos como paquetes de folios, ya que pueden propagar un incendio rápidamente. Sólo deberemos disponer en el centro computacional los necesarios para el buen funcionamiento de éste.

No podemos tener materiales inflamables de ningún tipo en nuestro centro computacional. En principio esta medida parece obvia, pero vamos a ver como no es tan extraño encontrar líquidos inflamables en nuestro centro computacional, ya que para la limpieza en general y para los equipos eléctricos en particular se emplean agentes que son altamente inflamables, como es el caso del alcohol o el amoniaco. Es importante que, aunque el uso a éstos se le vaya a dar en nuestro centro computacional, se almacenen fuera de éste y cuando se manipulen se haga con sumo cuidado.

c) Detectar un incendio en el centro computacional

Para detectar un incendio debemos emplear los detectores que hemos visto anteriormente, con la particularidad de que deben ser los indicados para el tipo de fuego que se pueda generar. Además deben situarse tantos como sea necesario, tanto manuales como automáticos, para detectar el incendio rápidamente. Vamos a verlo un poco más en profundidad.

i) Detectores manuales
La única diferencia con respecto al resto del edificio es que en el centro computacional debe existir, al menos, un avisador manual. Como hemos mencionado anteriormente, los avisadores manuales se deben colocar en los pasillos y rutas de escape hacia las salidas de emergencia, pero no en las salas u oficinas, a excepción de nuestro centro computacional.

ii) Detectores automáticos
De los detectores que hemos visto anteriormente, es posible que los más indicados sean los detectores iónicos, no obstante lo más importante en el centro computacional es que se **combinen varios tipos de detectores**, para cubrir todas las posibilidades y detectar el incendio lo más rápidamente posible.

d) Controlar un incendio en el centro computacional

Como ya hemos visto, para controlar un incendio es necesario definir correctamente los sectores de incendio. Puesto que un incendio se puede originar tanto en el interior como en el exterior de nuestro centro computacional, debemos definirlo como un sector de incendio independiente. De esta manera si el incendio se produce en el exterior evitaremos que se vea afectado, y si se origina en el interior se controlará mejor, por las medidas especiales de que disponemos en éste, si no sale del centro que si afecta a las zonas colindantes.

e) Extinguir un incendio en el centro computacional

Por la naturaleza de los dispositivos que tenemos en nuestro centro computacional es sumamente importante el elegir la técnica para sofocar el incendio y el agente para llevarla a cabo adecuados, ya que, como hemos mencionado, ciertos tipos de agentes extintores, como el agua o los polvos químicos, dejan, tras su aplicación, residuos que dañarían nuestros sistemas, tanto o más, que el propio incendio.

i) Técnicas
Por tanto, las técnicas que se deben emplear para apagar un incendio en nuestro centro computacional son por **enfriamiento** o por **sofocación** (supresión del oxígeno).

ii) Agentes extintores
Los agentes extintores que se pueden emplear en nuestro centro computacional son los **gases inertes** y los **gases halogenados**. El agua y la espuma son agentes conductores de la corriente eléctrica, por lo que nunca se deben emplear en nuestro centro computacional. Los polvos químicos no conducen la electricidad a tensiones normales, pero dado que los residuos que dejan pueden dañar los componentes eléctricos tampoco se deben emplear en nuestro centro computacional. Como ya hemos mencionado, los halones son altamente contaminantes, por lo que tampoco se pueden emplear como agente extintor en nuestro centro computacional y, en general, en ninguna zona del edificio.

iii) Cómo aplicar los agente extintores
La manera de aplicar estos agentes extintores puede ser mediante métodos manuales o automáticos. Para los métodos manuales emplearemos los **extintores portátiles**, cargados con el agente extintor adecuado. Dependiendo de las dimensiones de nuestro centro computacional, deberemos contar al menos con uno de éstos y cumplirá con las medidas que hemos visto anteriormente. No dispondremos de BIE´s en nuestro centro computacional, ya que el único agente extintor que pueden emplear es el agua.

En cuanto a los métodos automáticos, contaremos únicamente con **rociadores de agentes gaseosos**, por ser éstos los únicos que debemos emplear. Deberemos contar con un pulsador de activación manual y con otro de desactivación o retardo. Los rociadores pueden ser por inundación total, pero también debemos contar con rociadores por objetivo para los dispositivos más críticos.

e) Otros factores
Por ser especialmente críticos y delicados los dispositivos de que disponemos en nuestro centro computacional, existen otros factores en un incendio que debemos tener en cuenta a la hora de hablar de nuestro centro de cómputo, aunque los hayamos obviado anteriormente.

i) El humo

En un incendio se produce además una gran cantidad de **humo**, otra amenaza para nuestros sistemas. El humo, aparte de altamente tóxico, es un gran abrasivo. Es por ello que tras un incendio, aunque alguno de nuestros sistemas no se haya visto afectado por el fuego o el calor, deberá ser limpiado y comprobado en profundidad, ya que las partículas que el humo transporta se pueden depositar en nuestros dispositivos y

dejarlos inservibles, sobre todo las piezas móviles y las cabezas lectoras. Además el humo que se genera en un incendio es altamente abrasivo, por lo que puede dañar elementos como cables, sistemas de ventilación, aislamientos, etc.

ii) Contrarrestar las pérdidas

Dado el gran efecto que tiene el fuego sobre nuestros sistemas, se debe entender que es posible que aunque todos nuestros sistemas de prevención, detección y extinción funcionen al cien por cien, si se produjera un incendio, muchos de nuestros dispositivos queden destruidos. Es por ello que debemos contar con un **seguro** que cubra todos los daños materiales que nos pueda originar un incendio.

Como ya hemos mencionado, más críticos que los sistemas electrónicos en sí, son los datos que almacenamos en ellos. Por tanto, y como veremos más adelante, se debe contar con un sistema de **copias de seguridad** o backup que nos permita, en caso de una catástrofe, poder reanudar nuestro trabajo. Aunque hablaremos de esto en profundidad más adelante, por las consecuencias que puede tener para nuestra entidad un incendio y su extinción, es necesario mencionarlo en este punto.

iii) Conocimientos de cómo actuar ante un incendio

Como ya hemos comentado, es conveniente que algunos de nuestros trabajadores tengan conocimientos de cómo actuar ante un posible incendio. Por ser los elementos de que disponemos en el centro computacional especialmente críticos y los sistemas de extinción de incendios específicos para estos sistemas, será necesario que algunos si no todos los trabajadores que desarrollen su actividad diaria en el centro computacional tengan unas nociones básicas de cómo actuar ante un incendio, además de conocer perfectamente el funcionamiento de los sistemas antiincendios de que se disponen.

2.5.4 - El agua en el centro computacional

Como ya hemos mencionado en varias ocasiones, el agua es un gran enemigo de los sistemas eléctricos y, en general, de archivos, documentos, sistemas y dispositivos de almacenamiento, etc. es por ello que nuestro centro computacional es especialmente sensible a una posible inundación o fuga de agua. Por lo tanto se deben adoptar unas medidas de precaución extras, además de las que hemos aplicado al resto del edificio.

Las causas que hemos visto que pueden producir una fuga de agua, y por tanto una inundación, en el interior de nuestro edificio son por avería de desagües o grifos o por rotura de cañerías. El primer caso no debe preocuparnos en el centro computacional, puesto que no se deben tener grifos ni elementos que dispongan o precisen agua en el interior de éste. Además, como ya hemos comentado, su ubicación deberá estar retirada de baños, grifos, etc.

En el caso de rotura de cañerías, debemos verificar que no pasa ninguna cañería de agua por las inmediaciones de nuestro centro computacional. En el caso de que esto no se cumpla, se deberán tener perfectamente localizadas y se deberá contar con una llave que

permita, en caso de fuga, cortar el suministro de agua rápidamente y así evitar una posible inundación. Además se deberán situar detectores de agua cerca de las cañerías, sobre todo en las zonas poco visibles, para que en el caso de una fuga de agua se pueda actuar en consecuencia lo más rápidamente posible.

Una vez que hemos adoptado todas estas medidas la probabilidad de que se origine una inundación en nuestro centro computacional es muy reducida, por lo que tendremos que centrarnos ahora en que una inundación que se produzca fuera de éste no nos afecte. Para ello nuestro centro computacional debe estar aislado del resto de las instalaciones, mediante paredes, techos y suelos que resistan el paso del agua. Además de verificar que no pueda entrar agua por el hueco que queda entre falsos techos y suelos y el piso real.

Aún así, se deberán colocar sensores de agua en todas las zonas donde no se tenga visibilidad, como los mencionados huecos entre falsos suelos y techos y el piso real. Puesto que siempre existirán posibles accesos para el agua, como los puntos de acceso del personal, se deberán colocar sensores de agua cerca de éstos. Además nuestro centro computacional deberá contar con un desagüe, para que en caso de inundación el agua tenga una vía de salida.

2.5.5 - La humedad en el centro computacional

Otro factor a tener en cuenta en el centro computacional es el grado de humedad ambiental, puesto que un nivel alto de humedad en el ambiente puede provocar un mal funcionamiento de nuestros sistemas, incluso cortocircuitos por la condensación de ésta en el interior de los dispositivos eléctricos. Por el contrario, un ambiente extremadamente seco, o lo que es lo mismo, con poca humedad tampoco es propicio para nuestros sistemas, ya que favorece la aparición de electricidad estática, la cual puede dañar los dispositivos eléctricos. Por tanto, especialmente en nuestro centro computacional, **se deberá tener un grado de humedad adecuado, que oscilará entre el 45% y el 50%**, dependiendo siempre de las características concretas de los dispositivos de que dispongamos.

Dado que, como ya hemos comentado, el grado de humedad ambiental puede variar enormemente dependiendo de la época del año o de la zona geográfica en la que nos encontremos, es necesario que dispongamos de dispositivos en nuestro centro computacional que adecuen el grado de humedad ambiental al deseado. Estos dispositivos son automáticos y puesto que la humedad está muy ligada a la temperatura, estos dispositivos reguladores de humedad se encuentran normalmente integrados en los climatizadores. Si no disponemos de climatizadores o no integran un sistema de regulación de humedad, debemos instalar dispositivos de regulación de la humedad independientes. En cualquiera de los dos casos, estos sistemas constan de un **sensor de humedad**, un **humidificador** y un **deshumidificador**.

a) El sensor

El sensor detecta cuando el grado de humedad sobrepasa, por exceso o por defecto, unos límites establecidos. Cuando esto sucede, manda una señal, si se ha sobrepasado por

exceso al deshumidificador y si se ha sobrepasado por defecto al humidificador, activando su funcionamiento. Cuando el grado de humedad vuelve al rango admisible, vuelve a enviar una señal al sistema correspondiente deteniendo su funcionamiento.

b) El humidificador

Es el dispositivo que emplearemos para aumentar el grado de humedad del aire. Básicamente existen tres tipos de humidificadores, **fríos o ultrasónicos**, **calientes por electrodos** y **calientes por evaporación**.

i) Humidificadores fríos
Los humidificadores ultrasónicos, producen una nebulización del agua a través de vibraciones de muy alta frecuencia, son extremadamente seguros, silenciosos, con caudal regulable y de muy bajo consumo. Por otra parte sólo puede utilizarse agua y está absolutamente prohibido el uso de cualquier aditivo, como aceites u ambientadores. Su uso típico es la restauración de la humedad relativa durante largos períodos de tiempo. Son los más recomendados para nuestro caso.

ii) Humidificadores calientes por electrodos
Los humidificadores de electrodos generan vapor mediante la ebullición del agua del depósito calentada a través de la corriente que pasa directamente por el agua. Son más peligrosos ya que el vapor que expulsa lo hace a alta temperatura, y tienen un consumo elevado. El caudal de salida no es regulable y depende mucho de la dureza del agua. A mayor contenido de sales del agua mayor es la conductividad eléctrica y por tanto mayor la intensidad que circula, lo que a su vez implica un mayor caudal. Pueden emplearse con aditivos a la salida del vapor, nunca en el agua.

iii) Humidificadores calientes por evaporación
Los humidificadores por evaporación generan un caudal menor, no regulable y deben funcionar sólo con agua destilada. Su funcionamiento es mediante una mecha que se mantiene húmeda por capilaridad y que a su vez es calentada mediante un calefactor eléctrico. Si el agua contiene sales, la mecha se obtura con relativa facilidad. Pueden usarse con aceites balsámicos a la salida del vapor, pero su eficiencia en esto es muy inferior a la de los electrodos. Es el tipo menos usado.

b) El deshumidificador

Es el dispositivo que empleamos para reducir la humedad en el ambiente y consiste en una bomba de calor para proporcionar una zona fría donde condensar la humedad y una zona caliente para recuperar la temperatura ambiental. Su funcionamiento consiste en pasar una corriente de aire por el evaporador, la zona fría, el cual está a una temperatura por debajo de la de rocío, provocando que la humedad ambiental se condense en el evaporador y esta gotee a un depósito o un desagüe. Después de ser secado y enfriado el aire pasa por el condensador, la zona caliente, con lo que recupera la temperatura ambiental y disminuye aún más su humedad relativa.

A veces se puede producir hielo en la zona fría. En algunos aparatos, cuando detecta que la temperatura en la zona fría baja de 0 grados, se para la bomba de calor, pero se sigue moviendo el ventilador hasta que el hielo se derrita.

Debido a que el aire seco es más fácil de calentar y el proceso de condensar agua desprende calor, debido al calor latente de vaporización, la temperatura ambiente suele subir, por lo que se deberá contrarrestar este efecto con sistemas de aire acondicionado.

Como hemos visto, los humidificadores precisan agua para su funcionamiento y los deshumidificadores dejan como residuo agua, por lo que, tanto el abastecimiento de los humidificadores como el desagüe de los deshumidificadores, deben estar totalmente controlados y se deben adoptar las medidas que hemos comentado para el agua en el centro computacional, con el fin de evitar que ésta dañe nuestros sistemas.

2.5.6 - La temperatura en el centro computacional

La temperatura es un factor muy importante y que se debe tener muy en cuenta en nuestro centro computacional, puesto que influye enormemente en todos los dispositivos eléctricos, y especialmente en los electrónicos, como PC´s, servidores o dispositivos de red. Como ya hemos mencionado, una temperatura baja, incluso por debajo de cero grados, no afectará demasiado a nuestros sistemas, ya que éstos generan calor al funcionar, y es por esto precisamente por lo que las altas temperaturas sí les afectan.

Para disipar ese calor que generan los sistemas electrónicos se deben mantener a bajas temperaturas, para lo cual se implementan sistemas de ventilación o refrigeración especiales. Pero en muchas ocasiones, se requiere una investigación más profunda del tema, que puede ir desde el tipo de piso que se está ocupando a la cantidad de veces que se abre la puerta del recinto. Además, estos sistemas deben ser considerados como críticos, ya que si estos fallan y la temperatura supera un cierto valor, los sistemas eléctricos pueden quedar dañados permanentemente, lo que puede implicar la pérdida de datos.

Numerosas investigaciones han determinado que los equipos electrónicos que componen el centro computacional o sala de servidores deben tener una temperatura ambiente de entre 20 y 22 grados. Puesto que esta temperatura puede ser algo baja para los operarios que trabajan en el centro computacional, se puede disponer una separación física entre los servidores y *racks* más críticos, donde se mantendrá esta temperatura y las consolas para de operaciones, donde se encuentran los operarios y la temperatura puede ser algo más elevada, pero sin sobrepasar nunca los 27 grados centígrados. Esta separación física se puede implementar mediante mamparas de cristal, dejando siempre ver lo que ocurre al otro lado y sin interferir en los demás sistemas de seguridad, como los sistemas antiincendios o de control de la humedad.

El primer paso para implementar un sistema de refrigeración entonces es calcular la necesidad de enfriamiento que se requiere en el lugar determinado. Es importante en esta etapa no sobredimensionar la necesidad de enfriamiento, ni tampoco quedarse corto en capacidad. Vamos a ver, por tanto, unos **factores principales** que se dan en nuestro

centro computacional, **otros factores** que se deben tener en cuenta a la hora de implementar nuestro sistema de refrigeración y **los sistemas de refrigeración** para nuestros dispositivos.

a) Factores principales

Existen unos factores que se dan en todos los centros de cómputo y que se deben tener en cuenta a la hora de implantar un sistema de refrigeración, como elementos que generan calor, los empleados y su tránsito o la temperatura externa. Teniendo en cuenta estos factores se calcula la potencia de los sistemas de refrigeración que debemos instalar para funcionar en óptimas condiciones y bajo los estándares ideales de refrigeración.

i) Equipamiento

Entendemos por el equipamiento todos los sistemas que conforman nuestro centro computacional, como, por ejemplo, servidores, *racks*, monitores, SAI´s, etc. Es clave tener claro cuántos equipos se utilizarán en el centro computacional y qué cantidad de calor genera cada uno de ellos, independientemente de los sistemas de ventilación internos de que dispongan.

ii) Iluminación

La cantidad de luz y vatios de energía que existen en nuestro centro computacional también es un factor a considerar. Por lo general, lo ideal es utilizar sistemas de iluminación que liberen poca energía calorífica, como por ejemplo los tubos fluorescentes u otras tecnologías de luces frías.

iii) Número de empleados

El ser humano también genera una importante cantidad de calor, lo que influye en el promedio de temperatura ambiente ideal. Esto se torna más importante aún cuando existe una gran cantidad de operarios. Idealmente deberían ser pocos los operarios fijos en el interior del centro computacional, pero si por necesidades de la entidad esto no se puede, hay que calcular los sistemas de enfriamiento teniendo en cuenta el número de personas. Además, es importante destacar que este índice toma en cuenta también el flujo aproximado de personas que entra y sale del recinto.

iv) Luz solar

Aunque exista un excelente sistema de enfriamiento interno, la luz solar que llega directamente de las ventanas puede afectar a la climatización total o bien, a un área específica del centro computacional o, incluso, de un equipo en particular. Para evitar este problema se deben situar los sistemas fuera del alcance de los rayos solares que pudieran entrar por las ventanas. Hay que tener en cuenta que éstos varían dependiendo

de la época del año y de la hora del día. Si esto no fuera posible se deberán tapar las ventanas con elementos como persianas o simplemente prescindir de ventanas en nuestro centro computacional.

v) Apertura de puertas

Aunque parezca ridículo, la cantidad de veces que se abre una puerta también es un factor a considerar a la hora de mantener la temperatura ideal. Es muy importante para mantener la temperatura de nuestro centro computacional en los niveles deseados que éste sea una departamento aislado. Se debe procurar que la inmigración de temperatura sea la menor posible, para lo que se deben mantener las puertas cerradas tanto como sea posible.

vi) Temperatura externa

Aunque los sistemas y evaluaciones de enfriamiento modernos son capaces de implementarse bajo prácticamente cualquier realidad climática, siempre es recomendable tener en cuenta el clima existente en la localidad donde se encuentra el centro computacional, incluso la estación del año. No es lo mismo un servidor instalado en un país ecuatorial a uno que se encuentre en algún país escandinavo.

b) Otros factores a tener en cuenta

Existen, además, otros factores que se deben tener en cuenta a la hora de diseñar nuestro sistema de refrigeración del centro computacional.

i) Características de los sistemas

Es necesario conocer las características técnicas de todos los sistemas que tenemos en nuestro centro computacional, ya que puede que dispongamos de algún dispositivo que precise una temperatura especialmente baja (o alta) para funcionar correctamente. Si esto fuera así se tomarán las medidas oportunas.

ii) Previsión de crecimiento

Es deseable que la solución de refrigeración sea totalmente modular, es decir, que si instalamos nuevos servidores o PC´s podamos ampliar nuestro sistema de refrigeración para mantener las condiciones óptimas en el interior de nuestro centro computacional.

iii) Los sistemas de refrigeración son sistemas críticos

Puesto que hemos calificado nuestros sistemas de refrigeración como dispositivos críticos, deberemos cumplir ciertos requisitos de seguridad. Vamos a ver los más importantes.

iii.i) Disponibilidad
Los sistemas de refrigeración deben estar operativos constantemente, es por ello que para garantizar su continuidad deberán disponer de un sistema de alimentación eléctrica auxiliar, para que en caso de que falle la principal puedan seguir en funcionamiento, por lo menos, hasta que se hayan desconectado con seguridad todos los dispositivos del centro computacional.

iii.ii) Redundancia
Debemos contar con, al menos, un sistema auxiliar de refrigeración que permita, en caso de que el sistema principal falle, mantener una temperatura adecuada en el centro para desconectar con seguridad todos los sistemas sin que se vean afectados por un incremento de la temperatura.

iii.iii) Mantenimiento
Los sistemas de refrigeración precisan de unas revisiones y mantenimientos periódicos que vienen dados por las características técnicas concretas en cada caso. Estas revisiones deben ser realizadas por personal cualificado.

iv) Espacio y ubicación de los sistemas de refrigeración

El espacio y la ubicación son elementos importantes en una solución de refrigeración óptima, aunque muchas veces se dejan de lado. En muchas ocasiones se requiere de un sistema de refrigeración, pero en espacio reducido. Por esto, es importante que los equipos climatizadores sean poco invasivos y ocupen la menor cantidad de espacio posible, obviamente, dentro de ciertos márgenes. Es conveniente, además, que estos sistemas estén empotrados, manteniendo el equilibrio con la previsión de crecimiento.

v) Ruido y vibraciones

Puesto que los sistemas de refrigeración cuentan con partes móviles, producen en mayor o menor medida ruido y vibraciones. Aunque en el desarrollo de estos sistemas se preocupan cada vez más por reducir estos factores, se deben tener en cuenta. El ruido es un factor que, aunque puede resultar molesto para el personal que trabaje en el centro computacional, no interfiere con el resto de dispositivos. Por el contrario, las vibraciones puede que ni siquiera sean apreciables por los empleados, pero pueden dañar nuestros dispositivos, sobre todo sistemas de almacenamiento y cabezas lectoras.

vi) Caudal de aire

Aunque lo normal es que cada sistema de refrigeración en concreto tiene una disposición prefijada para optimizar su rendimiento, no hay que olvidar que el aire caliente sube mientras que el aire frío baja. Es por esto que si disponemos de varios dispositivos apilados unos encima de otros, por ejemplo, en un *rack*, los de la parte superior van a respirar el aire caliente que van expulsando los de la parte inferior.

vii) Sistema independiente

Es importante dejar claro que estamos hablando del sistema de refrigeración de nuestro centro computacional. Éste sistema debe ser totalmente independiente de los sistemas de climatización, refrigeración o calefacción que podamos tener instalados en el resto de nuestro edificio.

viii) Renovación del aire

El aire en nuestro centro computacional se debe renovar por completo entre 1,5 y 2 veces por hora. Con esta medida hacemos que el aire que del que disponemos en el centro de cómputo sea rico en oxígeno y, por un aumento de la presión, evitamos que entre aire sin haber sido tratado por puertas o ventanas.

c) Sistemas de refrigeración

Vamos a ver ahora de qué se compone y cómo funciona un sistema de refrigeración. Normalmente se cuenta con dos dispositivos en un centro computacional, un **sistema de aire refrigerado o acondicionado** y un **sistema de extracción de calor**. Éstos se complementan, por lo que se deben emplear conjuntamente.

i) Sistemas de aire refrigerado

Entendemos por sistemas de aire refrigerado los dispositivos que producen aire frío. Normalmente llamados **climatizadores**, estos sistemas no tratan el aire de ninguna otra manera que no sea su enfriamiento. Vamos a ver los elementos de los que están compuestos, su funcionamiento y su aplicación en un centro computacional.

i.i) Sistema de refrigeración
Es un artefacto metálico que cuenta con un líquido refrigerante encerrado en un circuito de cobre. El sistema hace que el líquido refrigerante cambie de presión y temperatura, por lo que tienen una cámara de frío y otra de calor. Por la cámara de frío pasa el aire que tomamos del exterior y se enfría para pasar a la canalización del aire. El aire caliente que se genera en la cámara de calor es expulsado. Puede generar como residuo cierta cantidad de agua. Por estos tres motivos, está situado en el exterior del edificio.

i.ii) Canalización del aire
Es un conducto desde el sistema de refrigeración hasta el dispensador de aire. Dependiendo de las necesidades variarán sus dimensiones. Generalmente son de aluminio.

i.iii) Dispensador de aire
Es la salida del aire frío. Está situado en nuestro centro computacional y cuenta con unos sistemas de orientación del aire para optimizar su rendimiento.

i.iv) Termostato

El termostato se encarga de regular la entrada de aire en función de la temperatura que haya en nuestro centro computacional. Es importante que el sensor del termostato esté situado lo más próximo a los sistemas que queremos refrigerar.

ii) Sistemas de aire acondicionado

La diferencia entre los sistemas de aire refrigerado y los de aire acondicionado es que en estos últimos el aire no es solamente enfriado, si no que además se controlan otros factores, como puede ser su pureza, su grado de humedad, su limpieza, y dependiendo del modelo en concreto, se podrá generar aire caliente en lugar de frío. Esto último no nos interesa en nuestro centro computacional.

El funcionamiento es básicamente el mismo que en el sistema de aire refrigerado, aunque, obviamente, los sistemas de aire acondicionado cuentan con más elementos, como pueden ser filtros de partículas, sensores de humedad, humidificadores y deshumidificadores, etc.

Generalmente, al igual que los sistemas de aire refrigerado, estos sistemas de aire acondicionado cuentan con termostatos digitales, con lo cual controlan la temperatura y la humedad, en su caso, de manera totalmente automática. No obstante, es conveniente monitorizar dichos factores con un sistema independiente a éste, lo que nos permita mayor veracidad en la toma de datos, redundancia y la posibilidad de actuar rápidamente si uno de estos factores está fuera del rango admisible para el buen funcionamiento de nuestros sistemas.

Puesto que la mayoría de sistemas de aire acondicionado cuentan con una pequeña consola para ajustar la temperatura a la deseada en cada momento, es importante mencionar que la temperatura de la zona donde se encuentren nuestros sistemas debe ser constante y regulada automáticamente. Haciendo uso de un ajusto manual sólo si por un fallo en el sistema automático se detecta una temperatura superior a la estipulada.

ii) Unidades extractoras de calor

Consisten simplemente en unos ventiladores que sacan el aire caliente de nuestro centro computacional al exterior, normalmente canalizado por tuberías. Es una solución económica diseñada para refrigerar *racks*. Por lo general, en este tipo de equipos, se puede ajustar de forma automática la velocidad de ventilación, basándose en el consumo de energía o temperatura. Además, se puede establecer la temperatura deseada y los ventiladores modificarán su funcionamiento automáticamente a fin de lograr la máxima eficiencia en el uso de la energía.

Estos sistemas garantizan la uniformidad de temperaturas entre los equipos montados en la parte superior del *rack* y los que se encuentran en la parte inferior. En algunos casos, según el fabricante, este producto, se instala en la parte posterior del gabinete,

ahorrando bastante espacio. Es posible encontrar *racks* que incluyen estos sistemas de refrigeración.

2.5.7 - El polvo en el centro computacional

Como ya hemos mencionado, el polvo es un gran enemigo de los sistemas electrónicos, y en particular de los dispositivos informáticos de que disponemos en nuestro centro computacional. Es por ello que se deben mantener estos dispositivos limpios y libres de polvo. Para lograrlo se debe evitar que entre polvo en nuestro centro computacional y, en su caso, evitar que se acumule.

Acabamos de ver que los sistemas de aire acondicionado que debemos instalar en nuestros centros de cómputo disponen de sistemas de tratamiento del aire para evitar que éste entre con partículas de polvo. En caso de no disponer de éste sistema, se deberá implantar uno independiente de purificación del aire. Sea como fuere, estos sistemas hacen pasar el aire por filtros, los cuales deben ser revisados y en su caso, sustituidos periódicamente.

Es importante también mantener nuestro centro computacional limpio, evitando así que el posible polvo que pueda acceder a la sala se acumule. En general, es especialmente importante seguir las pautas comentadas para el edificio con respecto al polvo en nuestro centro computacional.

2.5.8 - Vibraciones

Las vibraciones son otro factor que afecta muy negativamente a nuestros sistemas informáticos, especialmente a las cabezas lectoras, puesto que están calibradas con una precisión de micras.

Como ya hemos mencionado, las vibraciones pueden tener estar causadas por múltiples motivos. Ya hemos visto que pueden estar originadas por factores externos a nuestra entidad, en tal caso, deberemos alejar lo máximo posible nuestro centro computacional de la fuente de vibraciones.

Puede que existan dispositivos internos, como generadores de energía, sistemas de refrigeración o ventiladores que generen vibraciones. Deberemos tenerlos muy en cuenta y alejarlos lo máximo posible de nuestro centro computacional. Existen en el mercado espumas y aislantes especialmente diseñados para minimizar las vibraciones que provocan estos dispositivos. Es necesario, además, revisar que éstos funcionan correctamente, ya que si se encuentran en mal estado, puede que aún siendo perfectamente eficaces, generen una cantidad de vibraciones superior a la normal.

Los propios equipos de que disponemos en nuestro centro computacional generan vibraciones, puesto que incorporan ventiladores y piezas móviles, por lo que es necesario que los éstos se encuentren perfectamente asegurados en sus sustentáculos correspondientes, y que éstos estén a su vez fijados a las superficies fijas del centro computacional. Normalmente los dispositivos electrónicos vienen provistos de unas gomas que se adhieren a la parte inferior de éstos para aislarlos unos de otros y de las

superficies fijas, y así reducir la cantidad de vibraciones. En caso de que esto no fuera así, deberemos disponerlas nosotros mismos. En casos extremos, existen otras medidas más radicales, como son el uso de gomas o soportes especiales que eliminen por completo las vibraciones en los equipos.

2.5.9 - El personal en el centro computacional

Es necesario mencionar que es muy posible que a nuestro centro computacional no accedan solamente los administradores de los sistemas, si que puedan o deban acceder a éste otros grupos de personas que veremos a continuación.

a) Administradores

Los administradores del sistema, y los empleados en general, que desarrollen su actividad diaria en el centro computacional son las personas que más concienciadas con la seguridad deben estar, puesto que en gran medida van a ser los responsables de hacer que las medidas que hemos estado comentando se cumplan.

b) Empleados

Es normal que en ciertas ocasiones trabajadores que no desarrollan su actividad cotidiana en el centro computacional tengan que acceder a éste, incluso que durante un periodo de tiempo accedan regularmente. Se deberá valorar si se les habilita el acceso al centro o si por el contrario accederán a éste cuando los administradores estén dentro.

c) Empleados de limpieza

Un factor muy a tener en cuenta es la limpieza del centro computacional, ya que como hemos visto, es algo muy importante para un buen número de medidas de seguridad. El personal de limpieza, sea de la propia entidad o externo, deberá firmar unas cláusulas de confidencialidad para evitar que puedan filtrar información de nuestro centro computacional. Por supuesto, deberán estar al tanto de los sistemas de seguridad para no provocar el fallo de ninguno y se deberá valorar si ejercen su labor en horas de oficina, con el personal trabajando en el centro computacional o si lo hacen fuera de estas horas. En el primer caso puede que trabajadores y personal de limpieza se entorpezcan mutuamente, pero estarán más controlados.

d) Personal de mantenimiento

Existen múltiples dispositivos que requieren un mantenimiento periódico por parte de personal calificado ajeno a la entidad. Incluso pequeñas modificaciones en nuestro centro computacional requerirán que trabajadores externos accedan a éste. Por tanto se deberá establecer una política de actuación, es decir, si pueden acceder sólo acompañados por empleados o vigilantes de seguridad, qué horarios son los adecuados, si deben firmar cláusulas de confidencialidad, etc.

2.5.10 - La basura

Normalmente por basura entendemos desperdicios de cualquier tipo sin ningún valor. Cuando hablamos de la basura que se genera en un centro computacional la cosa es muy distinta, ya que los desperdicios que se generan en un centro computacional son normalmente documentos con información muy valiosa para la entidad. Estos documentos pueden ser desde datos de los empleados, como nombres, teléfonos, contraseñas de red, etc. hasta esquemas de la estructura de red, políticas de seguridad o fragmentos de código fuente. Obviamente si estos datos llegaran a manos inadecuadas podrían poner en grave peligro la seguridad de la entidad.

Por tanto, todos los documentos que hayan perdido su utilidad para la entidad y que no estén debidamente almacenados y bajo determinadas medidas de seguridad, deben ser destruidos. Puesto que la criticidad de estos documentos es muy alta, no podemos dejar posibles puertas abiertas a la reconstrucción de los documentos, por tanto debe ser imposible la reconstrucción de los documentos tras su destrucción, obviamente la mejor solución para tal fin es la **incineración**. Es conveniente, y de no se aplicarse otros sistemas de destrucción, contar en nuestro centro computacional con un **destructor de papel**.

En el caso de almacenamiento en soporte informático, no basta con borrar los documentos, puesto que existen sistemas capaces de recuperar información de discos que han sido incluso formateados, por lo que se debe contar con una **aplicación de borrado seguro**. Existen **empresas que se dedican a la destrucción segura** de elementos de este tipo, puede ser una buena opción contratar sus servicios. Es conveniente, además, llevar un control de todos los elementos que se eliminan.

Vamos a ver los principales elementos que pueden albergar información sensible para la entidad y que deben pasar por un proceso de eliminación antes de ser desechados.

i) Documentos en papel
Toda clase de documentos que podamos tener en nuestro centro computacional, desde fichas de empleados, clientes o proveedores, pasando por datos técnicos de nuestros sistemas hasta esbozos de la configuración de nuestra red interna.

ii) Voces u otras grabaciones
En muchas ocasiones, en las entidades se graban reuniones o acuerdos en dispositivos como magnetófonos o grabadoras digitales. Esto puede ser una fuente de información muy valiosa.

iii) Papel carbónico
Para realizar copias de documentos es usual emplear el papel carbónico. Tras su utilización puede quedar marcado todo lo que se ha copiado con él.

iv) Informes de salida
En muchas ocasiones se realizan informes rutinarios que pueden carecer de valor transcurrido un cierto tiempo, pero siguen albergando datos sensibles para la entidad.

v) Cintas de impresora de un solo uso
Ocurre lo mismo que con el papel carbónico, tras su utilización pueden quedar grabados en éstas todos los datos que han copiado.

vi) Cintas magnéticas
Las cintas magnéticas son un elemento principal de almacenamiento de datos, sobre todo para hacer copias de seguridad. Si una de éstas quedara dañada, hay que tener presente que puede seguir albergando toda o parte de la información que se había grabado.

vii) Disquetes
Aunque la capacidad de los disquetes es muy reducida, aún hoy en día se siguen empleando. Puesto que se estropean con gran facilidad, hay que desecharlos de forma segura.

viii) Medios de almacenamiento óptico
Es otro sistema de almacenamiento, como CD´s o DVD´s. Tienen gran capacidad y pueden albergar una gran cantidad de datos, por lo que se deben destruir antes de ser desechados.

ix) Datos de prueba
En muchas ocasiones se generan datos de prueba para depurar sistemas informáticos. Aunque aparentemente estos datos no parezcan importantes, en manos expertas pueden facilitar mucha información.

x) Documentación del sistema
Los sistemas de que disponemos deben estar muy documentados, para facilitar su uso. Ésta documentación puede facilitar información importante acerca de nuestros sistemas.

Al acopiar medios para su eliminación, se debe considerar el efecto de acumulación, que puede ocasionar que una gran cantidad de información no clasificada se torne más sensible que una pequeña cantidad de información clasificada.

Además debe de crearse una política de destrucción de documentación que todos los empleados deberán cumplir, responsabilizándose cada uno de los datos y documentación que desechen.

2.5.11 - Comida y bebida

Uno de los mayores factores de riesgo para causar accidentes es la comida y la bebida. Al igual que el agua, se corre el riesgo de derramar el líquido sobre el equipo, especialmente sobre el teclado, provocando su inoperatividad. Con la comida sucede lo mismo, especialmente con la comida grasienta. La grasa se acumula en los dedos de las personas y las migas son residuos que se acumulan sobre todo en los teclados de los equipos. La mejor solución, pese a ser algo muy estricto, es mantener la comida alejada de los ordenadores, por lo que se debe prohibir entrar en el centro computacional con comida o bebida.

Otro factor importante es que tanto la comida como la bebida pueden atraer visitantes no deseados al centro computacional, como ratas, ratones, hormigas, cucarachas y todo tipo de insectos en general. Aparte del contratiempo y malestar que puede suponer para los trabajadores del centro computacional, pueden introducirse en los dispositivos, deteriorar los cables o cualquier elemento en general, dejándolo inservible o provocando su malfuncionamiento.

2.5.12 - Armarios de seguridad

Puesto que en el centro computacional contaremos con elementos especialmente sensibles o críticos, es necesario que contemos con **armarios de seguridad**. Existen distintos tipos de armarios de seguridad, dependiendo del modelo en concreto los riesgos contra los que nos pueden proteger.

Es necesario que estos armarios cuenten con un sistema de apertura que garantice que un intruso que accede al centro computacional no podrá abrirlas, ya sea mediante cerraduras con llave, mecanismos de apertura mediante una combinación de números o por algún sistema digital de validación ya mencionados en este trabajo.

Como ya hemos comentado, estos armarios deben proteger su contenido de las altas temperaturas que se puedan originar en un incendio, así como de una posible inundación.

Sólo se debe guardar en estos armarios los elementos especialmente sensibles o críticos, por su valor económico o por su importancia para el funcionamiento de la entidad, que hemos comentado, tales como copias de seguridad, software o hardware suficientemente importante o esquemas o documentos los cuales sea necesaria su presencia en el centro computacional.

2.6 - Copias de seguridad o backups

Como hemos venido viendo durante todo el trabajo, la información que se maneja en una entidad hoy en día es posiblemente su activo más valioso, ya que en muchos casos esta información ha sido creada en la propia entidad como fruto del desarrollo continuo de ésta. Incluso la pérdida de aplicaciones adquiridas puede suponer un gran contratiempo, ya que la puesta a punto y configuración concreta para nuestra entidad ha podido suponer un gran esfuerzo para nuestros trabajadores. Por este motivo, no existe ninguna fuente externa de la que podamos valernos para recuperar la información en caso su pérdida. Existen múltiples motivos por los que podemos perder toda o parte de la información, desde grandes catástrofes, como incendios o inundaciones, pasando por robos o sabotajes, hasta fallos en los sistemas o dispositivos de almacenamiento.

Por tanto, parece obvio que se tienen que tomar ciertas medidas especiales para que, en caso de un desastre en el que perdamos la información que tenemos almacenada en nuestros PC´s o servidores, podamos recuperarla. Para ello debemos realizar copias de seguridad de toda la información, a las que como hemos comentado anteriormente, se las denomina backups.

2.6.1 - Backups del sistema y backups de datos

La primera diferencia entre copias de seguridad está entre las copias de seguridad de datos y las copias de seguridad del sistema. A la hora de realizar una copia de seguridad de nuestro sistema deberemos decidir si salvaguardamos todo lo que tenemos en éstos, como sistemas operativos aplicaciones y datos o si solamente la realizamos de los datos. Vamos a ver las ventajas y desventajas de cada tipo.

a) Backups del sistema completo

Hacemos una copia de seguridad de todo nuestro sistema, incluyendo sistema operativo, aplicaciones, datos, configuraciones, etc. Este tipo backup tiene la ventaja de restaurar el sistema desde las copias de seguridad tras una pérdida de información será un proceso más rápido y fiable. Por el contrario, mantener las copias de seguridad actualizadas requiere un mayor esfuerzo y el volumen de datos que se maneja es mucho mayor.

b) Backups de datos

Cuando realizamos las copias de seguridad lo hacemos sólo de los datos que albergamos en nuestros sistemas, como bases de datos, documentos, correos electrónicos, etc. El volumen de datos que se maneja es mucho menor que en el tipo de backup anterior y resulta más sencillo mantenerlo actualizado, pero por el contrario, a la hora de restaurar nuestro sistema desde el backup necesitaremos emplear más tiempo y esfuerzo.

2.6.2 - Tecnologías de backups

La tecnología empleada para llevar a cabo copias de respaldo depende esencialmente de la importancia de los datos a respaldar. Bajo este criterio es necesario mantener un equilibrio entre **el volumen de datos a tratar**, **el coste económico de los medios de almacenamiento** y **la operatividad de la solución en cuanto a tiempo de copia y recuperación**. Así, existen dos soluciones típicas, no son excluyentes sino complementarias.

a) Copia en línea

La copia en línea consiste en replicar la infraestructura de almacenamiento principal en una infraestructura secundaria. Esto es, los discos corporativos principales se replican generalmente en un centro de respaldo. El centro de respaldo es un sistema donde se van almacenando directamente los datos provenientes de la estructura principal. Dependiendo de las necesidades y el volumen de datos, el centro de respaldo puede ser desde un PC conectado a la Internet hasta un sistema de discos magnéticos de alto rendimiento conectado directamente al sistema principal mediante fibra óptica. Es evidente que el centro de respaldo debe contar con hardware y software totalmente compatible con el del centro computacional, incluyendo mismas versiones y parches, ya que si no, no se podrá garantizar la integridad de los datos copiados.

Un sistema de backup basado en esta tecnología debe garantizar unas necesidades de disponibilidad y servicio suficientes, por lo que vamos a tratar solamente los sistemas de **discos magnéticos de alto rendimiento** conectados por un enlace directo al sistema principal, generalmente de **fibra óptica** o **SCSI**. Existen además dos sistemas de copiado en línea, inmediato o asíncrono.

i) Copiado inmediato
Los datos se copian inmediatamente después de ser creados o modificados en el centro de cómputo principal. Hasta que esto no se lleva a cabo no se continúa realizando ninguna otra operación. La probabilidad de que se pierda algún dato es casi nula, por lo que es un sistema idóneo para entidades que realizan multitud de operaciones críticas, como un banco, donde no se puede perder ninguna transacción económica que se realice. Este sistema requiere una comunicación inmediata entre el centro computacional y el centro de respaldo, además de una respuesta inmediata de éste, por lo que es un sistema muy caro.

ii) Copiado asíncrono
Es similar al anterior, pero en este caso, los datos al ser creados o modificados en el centro computacional se almacenan en éste y se envían al centro de respaldo cada cierto tiempo, desde unos pocos minutos hasta varios días, en bloques de mayor tamaño. Cuanto menor sea el tiempo entre envío de datos, más actualizada y fiable será la copia de seguridad. Es un sistema más barato que el anterior, ya que no requiere una respuesta inmediata y es el adecuado para centros donde es más importante la continuidad del negocio que las propias operaciones que se realizan, como es el caso de un hipermercado.

Para conseguir un mejor equilibrio en costes es posible habilitar un segundo nivel de almacenamiento compuesto por discos más baratos, generalmente ATA o SATA. Los datos más antiguos o menos utilizados se mueven a este segundo nivel liberando espacio de los discos más caros.

El centro de respaldo debe estar a una cierta distancia del centro computacional principal, con el fin de que una misma contingencia no afecte a ambos. Esta distancia estará limitada por las necesidades de telecomunicación entre ambos centros.

b) Copia fuera de línea

La copia fuera de línea consiste en duplicar los datos afectados en medios de almacenamiento intercambiables. Generalmente, cintas magnéticas, pero también DVD´s, discos duros o cualquier otro medio de los que veremos a continuación. Todos éstos se caracterizan porque necesitan ser físicamente montados en los lectores antes de poder ser utilizados.

Se trata de una solución barata pero lenta de recuperar. Ya que los datos pertinentes deben ser primero localizados en el medio físico que los contiene, montados físicamente en un lector, y restaurados. Generalmente, las velocidades de transferencia de estos medios son sensiblemente inferiores a las de un disco corporativo.

La principal ventaja es que los datos están salvaguardados en un medio físico de reducido tamaño, fácilmente transportable e independiente, con lo que se puede almacenar en cualquier lugar seguro, alejado del centro de cómputo principal.

Como es evidente, las copias de respaldo deben realizarse en momento en que los datos principales no están siendo modificados y se encuentren en una situación estable. Por ello, es necesario esperar a que las aplicaciones que los manejan dejen de utilizarse. Generalmente, al terminar la jornada laboral.

Por otra parte, la copia de respaldo tiene una limitación en velocidad de transferencia. De manera que a mayor volumen de datos, más tiempo se necesita para realizar cada copia. La franja horaria en la que es posible realizar copias de respaldo se denomina **ventana de backup** y supone un límite a las políticas y estrategias de copia. Para mantener el tiempo de copia dentro de la ventana de backup existen diversas opciones. Vamos a ver además las diversas políticas de copiado existentes.

i) Métodos para reducir el tiempo de copiado

i.i) Reducir el volumen de datos a copiar
Generalmente, copiando únicamente aquellos datos que hayan variado respecto a una copia anterior.

i.ii) Aumentar artificialmente la ventana de backup
En cabinas de discos corporativos es posible generar una "copia congelada" *(snapshot)* de los datos gracias a la estrategia *copy on write*. Los dispositivos de respaldo trabajan con una copia ficticia mientras las aplicaciones siguen trabajando con los datos reales.

i.iii) Mayor velocidad de transferencia
Utilizar dispositivos con mayor velocidad de transferencia a medida que mejora la tecnología.

i.iv) Combinar copia en línea y fuera de línea.

ii) Políticas de copiado

Por otro lado, cuando se utilizan medios de almacenamiento fuera de línea existen tres políticas ya consagradas

ii.i) Copia total
Consiste en una copia completa de todos los datos principales. Requiere mayor espacio de almacenamiento y ventana de backup.

ii.ii) Copia diferencial
Consiste en copiar únicamente aquellos datos que hayan sido modificados respecto a una copia total anterior. Requiere menor espacio de almacenamiento y ventana de backup. Para restaurar una copia diferencial es necesario restaurar previamente la copia total en la que se basa. Por tanto, requiere mayor tiempo de restauración. Una copia

diferencial puede sustituir a otra copia diferencial más antigua sobre la misma copia total.

ii.iii) Copia incremental
Consiste en copiar únicamente aquellos datos que hayan sido modificados respecto a otra copia incremental anterior, o bien, una copia total si ésta no existe. Nótese que una copia incremental no sustituye a las copias incrementales anteriores. Para restaurar una copia incremental es necesario restaurar la copia total y **todas** las copias incrementales por orden cronológico que estén implicadas. Si se pierde una de las copias incrementales, no es posible restaurar una copia exacta de los datos originales.

2.6.3 - Medios donde realizar backups fuera de línea

Una cuestión a tener en cuenta con los sistemas de backup es el medio donde se realizan los backups. Puesto que un backup es una copia de cierta información, en principio se podrán realizar en cualquier dispositivo de almacenamiento, desde un disquete hasta un servidor remoto, pasando por un DVD. Sin embargo existen ciertos sistemas específicos para realizar backups a gran escala, como son las **cintas de backup**, las **cintas DAT** y los **discos ZIP**, ya que están especialmente diseñados para ello.

i) Disquetes

Por su capacidad tan limitada, 1,44 MB, únicamente se podrán hacer copias de pequeños documentos (no entran en la definición de copias de seguridad a gran escala) y normalmente a nivel de usuario final. Con el tiempo pierden la información que almacenan y son muy sensibles a las ondas electromagnéticas, como las producidas por los teléfonos móviles. Para su utilización es necesaria únicamente una disquetera en un PC. Hoy en día existen alternativas suficientes como para que su uso esté abolido.

ii) Sistemas de almacenamiento ópticos

Los sistemas de almacenamiento ópticos son los CD´s y DVD´s. Tienen capacidad para albergar una cantidad de información mucho mayor que los disquete, hasta 800MB y hasta 9GB, respectivamente, pero tienen una vida corta y son bastante delicados. Sin embargo, dada su gran disponibilidad y facilidad de uso, y puesto que solo se necesita una grabadora montada en un PC para su utilización, se podrán emplear para realizar copias y como sistemas de almacenamiento secundario, pero siempre que se disponga además de otro sistema especifico de backup.

iii) Discos duros convencionales

Otra posibilidad es realizar copias en discos duros. Éstos pueden tener una gran capacidad de almacenamiento, hasta 500GB, pero son muy delicados a los golpes y movimientos bruscos. Al igual que los sistemas ópticos, pueden servir como dispositivos de almacenamiento secundario, pero nunca como un sistema único de

backup. Pueden ser externos o internos, y su funcionamiento requiere únicamente un PC, por lo que es un mecanismo con una gran disponibilidad.

iv) Servidores

Un sistema para realizar copias de seguridad es empleado un servidor de datos. En definitiva, la información se almacenará en un disco duro, pero se enviará la información que queremos copiar por medio de la red, interna o externa, hasta el servidor. Este sistema depende por tanto de la disponibilidad de la red para mantenerse operativo, además de tener una velocidad de transmisión limitada, por lo que no se podrán emplear con un gran volumen de datos.

v) Discos ZIP y JAZ

Los discos ZIP son unos cartuchos, similares a los disquetes convencionales, pero tienen una capacidad de almacenamiento mucho mayor, hasta 200MB. Son más resistentes y seguros, pero su tecnología está algo obsoleta y son sensibles a las ondas electromagnéticas. Para su funcionamiento requieren un dispositivo lector-grabador montado en un PC. Tienen una gran disponibilidad, por lo que es un buen mecanismo para realizar backups de pequeños volúmenes de información y como elemento secundario de almacenamiento. Los JAZ son casi idénticos, pero cuentan con una tecnología más moderna por lo que pueden albergar hasta 2GB.

vi) Cintas magnéticas de backup

Las cintas magnéticas son el soporte más empleado hoy en día, puesto que está especialmente diseñado para este fin. Son muy resistentes a golpes y movimientos bruscos, sin embargo se pueden ver afectadas por radiaciones electromagnéticas. Tienen la característica de que es un soporte secuencial, es decir, que para encontrar un dato que tengamos guardado en la cinta tendremos que recorrer el soporte hasta encontrarlo, no pudiendo acceder hasta él directamente, como en los medios que hemos visto anteriormente.

Precisan de un lector-grabador para grabar y leer los datos. Existen modelos que tienen capacidad para varias cintas y el sistema se encarga de manejarlas automáticamente. Existen varios tipos de cintas magnéticas, todos ellos muy parecidos, **las DAT**, **las DLT** y las ***Ultrium-II***, este último es el más empleado hoy en día, aunque todos son muy similares. La capacidad de cada cinta puede variar dependiendo del tipo y del modelo en concreto, pero generalmente está entre 10GB y 500GB. Algunas tecnologías ofrecen la posibilidad de almacenar los datos comprimidos, lo que aumenta la capacidad del cartucho.

2.6.4 - Reutilización del medio de almacenamiento

Como ya hemos comentado, las copias de seguridad se pueden realizar en muy diversos soportes de almacenamiento. Algunos de estos soportes son de un solo uso, como los

CD´s o DVD´s, por la gran mayoría se pueden reutilizar, sobrescribiendo datos nuevos en los antiguos. Es importante conocer cuantas veces podemos sobrescribir en un determinado soporte sin que éste pierda las cualidades necesarias para garantizar la integridad de los datos almacenados. Esta información la obtendremos en los manuales de uso de cada dispositivo en concreto.

Para la reutilización de los soportes debe existir un control que garantice el seguimiento de todos los datos almacenados. Además se debe crear una política sobre cuanto tiempo tendremos un soporte almacenado sin rescribirlo para garantizar que se podrá recuperar la información necesaria.

Una política muy empleada hoy en día es rotar los soportes con distintos intervalos, anual, mensual, semanal, etc. Aunque depende en gran medida de los dispositivos de almacenamiento empleados y de las necesidades de la entidad.

2.6.5 - Funcionalidad de los sistemas de backup

Aunque parece algo obvio, de nada nos sirve hacer copias de seguridad si cuando necesitamos usarlas para restaurar el sistema tras una pérdida de información no funcionan. Por tanto, algo muy importante es comprobar que las copias de seguridad que hemos realizado pueden ser restauradas correctamente. Para ello se deben hacer restauraciones de prueba, incluso periódicamente, para asegurarnos de que podemos confiar plenamente en nuestro sistema de backup.

2.6.6 - Seguridad física de las copias de seguridad

Parece obvio que por la importancia de estos dispositivos deben mantenerse bajo unas medidas de seguridad física apropiadas, vamos a ver los tres motivos principales y qué medidas especiales se deben tomar.

i) Factores que deben cumplir los backups

i.i) Confidencialidad de los datos
Ya que en estos dispositivos almacenamos toda la información de nuestra entidad, por lo que es necesario que nadie, excepto nosotros mismo, tenga acceso a la misma.

i.ii) Disponibilidad de los datos
Puesto que las copias de seguridad pueden ser necesarias en cualquier momento, necesitamos que estén siempre disponibles para ser usadas.

i.iii) Integridad de los datos
Los datos que almacenamos en los dispositivos de backup no pueden sufrir alteraciones de ningún tipo, para ello estos dispositivos deben estar a salvo de los elementos que les podrían causar algún daño, como radiación electromagnética, humedad, radiación solar, etc. dependiendo del dispositivo en concreto.

ii) Medidas de Seguridad Física que debemos adoptar

Lo primero que tenemos que comentar es que como los elementos críticos para la entidad que son, deben tomarse las medidas de seguridad correspondientes. Vamos a ver a rasgos generales algunas peculiaridades de los sistemas de backup.

ii.i) No almacenarlos en el propio centro computacional
Como ya hemos comentado anteriormente, para que una situación que afecte a nuestros sistemas de almacenamiento de datos principales no lo haga a los sistemas de backup, éstos deben estar almacenados a una distancia suficiente del centro computacional, generalmente, en otro edificio. Puesto que no todas las entidades cuentas con varios edificios en su haber, existen empresas que se dedican a la recogida y almacenaje de dispositivos de backup, garantizando todas las medidas de seguridad necesarias.

ii.ii) Condiciones ambientales adecuadas
Como ya hemos mencionado, el ambiente donde se almacenen los dispositivos de backup debe ser el adecuado para mantener la operatividad de éstos. Estas condiciones las indica el fabricante para cada dispositivo concreto y los factores principales a tener en cuenta son radiación electromagnética, como la provocada por teléfonos móviles, humedad, radiación solar, temperatura y vibraciones, entre otras.

ii.iii) Redundancia de backups
Otra medida de seguridad que se debe tomar es la redundancia de las copias de seguridad, es decir, realizar, por lo menos, dos copias en lugar de una y almacenarlas en lugares distintos. De esta manera estaremos solventando dos problemas. Por un lado podremos disponer de dos fuentes distintas para recuperar nuestros sistemas en caso de que sea necesario, y por otro aumentaremos la disponibilidad de los backups, ya que podremos almacenar esta segunda copia en nuestro centro computacional, con lo que podremos disponer de ésta en el caso de que sea necesario más rápidamente.

3 - AUDITORÍA INFORMÁTICA

3.1 - Introducción

3.1.1 - Definición

Hace unas décadas el término **auditoría** se asociaba exclusivamente a la revisión de cuentas y estados financieros. En 1971 Thomas Porter daba una definición de auditoría muy general, sin hablar en ningún momento de cuentas o finanzas. Sin embargo, el REA (Registro de Economistas Auditores) sí que daba una definición de auditoría mucho más concreta, refiriéndose exclusivamente a estados financieros es particular, por no haber ido surgiendo ningún otro tipo de auditoría.

Hoy en día la definición que da la Real Academia Española da la siguiente definición de auditoría:

> *"Revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse"*

Una definición muy general, y que por tanto podemos aplicar a cualquier actividad, no exclusivamente a las cuentas o finanzas.

Aunque ya en 1969 se había creado ya la EDPAA (*Electronic Data Processing Auditors Association* - Asociación de Auditores de Procesos de Datos Electrónicos), hoy ISACA, no existe una definición *oficial* de auditoría informática, y algunas de las que aparecen en libros o se dan en cursos o seminarios no son adecuadas, ya que el concepto que tienen muchos profesionales es el de *auditoría de cuentas con ayuda del ordenador*. Si bien es claro que **el objeto a examinar** en este caso son los estados contables o los balances entre otros documentos, empleando como **herramienta** algún sistema informático.

Por tanto, en la auditoría informática el objeto a analizar son los propios sistemas informáticos, empleando para ello herramientas informáticas o no. Con todo esto podemos decir que **la auditoría informática *es la revisión de la propia informática y de su entorno***, lo cual no implica que se tenga que usar el ordenador para ello. Además, la revisión que se debe llevar a cabo en cualquier campo debe ser una revisión que se lleve a cavo desde **un punto de vista independiente y objetivo**, profundizaremos en esto más adelante.

Podemos añadir también que la auditoría consiste en *comparar lo que existe con lo que debería existir y lo que se hace con lo que se debería hacer*.

3.1.2 - Ámbito de actuación

Algo muy común es relacionar la auditoría informática con la auditoría de la seguridad. Aunque en este trabajo vamos a tratar la **auditoría de la seguridad física de los sistemas de información**, no debemos confundir estos dos conceptos, puesto que la

auditoría informática puede abarcar muchas otras áreas. De hecho es difícil determinar que áreas puede abarcar y cuales no, ya que incluso podríamos auditar la gestión de la propia informática. Por tanto, la delimitación de hasta donde debe llegar la auditoría informática depende del objetivo de ésta, pudiéndose modificar, incluso, en el desarrollo de ésta si se creyera conveniente.

Otro aspecto a tener en cuenta es que la auditoría informática no se limita únicamente a los PC´s, como mucha gente piensa, si no también a su entorno y elementos igualmente importantes, como servidores de datos, canales de comunicaciones, etc. dependiendo de la profundidad y el objetivo de dicha auditoría.

3.1.3 - Regulación

Sería más adecuado hablar de **ausencia de regulación,** puesto que no existe en España ninguna normativa relacionada con la auditoría informática, de hecho, no todos los profesionales que realizan auditorías informáticas tienen la formación y experiencia deseables para que puedan llevar a cabo su trabajo con ciertas garantías.

Por este motivo, no hay una definición oficial de quién debe realizar las auditorías, de cómo realizarlas ni de en qué casos es necesaria. Puesto que esto si está regulado en el caso de las auditorías de cuentas, y dado que hoy en día la gran mayoría de los entornos cuentan con equipos y sistemas informáticos para su gestión, una de las utilidades de la auditoría informática es la de apoyo a la regulada auditoría de cuentas.

3.1.4 - Auditoría y consultoría

Existe también una cierta confusión entre estas dos actividades. Es evidente que tienen muchos aspectos y requisitos comunes, pero debemos ver las diferencias entre ambas. Mientras que en la auditoría vamos a **analizar y evaluar** las posibles deficiencias o errores para emitir un informe con las posibles soluciones, en la consultoría se va a dar una mejor **definición de** esas **soluciones, participando en** la mayoría de casos en su **implantación**, desarrollando aplicaciones, configurando los sistemas o aplicando determinadas medidas de seguridad. Por tanto, el objetivo de estas dos actividades es distinto.

3.2 - Tipos de auditoría informática

Podemos hablar de dos maneras de clasificar la auditoría informática, atendiendo a su **objeto** o atendiendo a su **origen**.

3.2.1 - Atendiendo al objeto

Obviamente, podremos diferenciar los distintos tipos de auditoría informática atendiendo al objeto que tienen, o más concretamente, la profundidad de ésta. Sin embargo esta clasificación no se emplea normalmente, ya que existe una gran variedad de objetivos a analizar y por tanto es difícil dar clasificación formal, además de que

unos pueden englobar a otros. Podemos hablar, no obstante, de las siguientes las siguientes clases de auditoría.

a) Evaluación del sistema de control interno

b) Auditoría del cumplimiento de estándares, políticas y procedimientos de la propia entidad, así como de normas legales aplicables, etc.

c) Auditoría de la seguridad lógica

d) Auditoría de la seguridad física

e) Auditoría operativa o de gestión

f) Auditoría informática como apoyo a la auditoría de cuentas

g) Investigación de delitos informáticos

3.2.2 - Atendiendo al origen

Esta es una clasificación mucho más interesante, puesto que existe una diferencia mucho más tangible entre los dos tipos que existen. Estos dos tipos de auditoría informática son **auditoría informática interna** y **auditoría informática externa**.

a) Auditoría informática interna

Es la auditoría informática que es llevada a cabo por un departamento de la propia entidad a auditar. Como ya hemos comentado, la auditoría informática debe llevarse a cabo desde un punto de vista objetivo e independiente, por tanto el departamento y el personal que lo forme deben cumplir una serie de requisitos para la auditoría sea efectiva y fiable. Para ello podemos optar por personal proveniente de la propia entidad o externo a ésta. Vamos a ver los principales aspectos a tener en cuenta.

i) Dependencia jerárquica del departamento
El departamento debe depender directamente del director general o del comité de administración de primer nivel en la entidad o de un auditor general, pero nunca de otro departamento y en especial del departamento de informática o de su director.

ii) Empleados provenientes de otros departamentos
Si el departamento está formado por empleados que antes habían trabajado en otros departamentos, especialmente en el de informática, se puede dar el caso de que deban auditar antiguos trabajos o proyectos realizados por ellos mismos, lo que va a condicionar su evaluación de los mismos.

iii) Relación entre trabajadores
Otro factor importante es que los trabajadores del departamento de auditoría deban auditar a empleados con los que tienen en mayor o menor medida una relación, tanto

profesional como de cualquier otro tipo. Éste motivo también puede ser causa de una valoración no objetiva.

iv) No realizar otras funciones
Algo muy importante es que los empleados que conformen el departamento de auditoría no realicen ningún otro tipo de funciones en la entidad.

Como hemos comentado, para conformar dicha plantilla podemos optar por contratar gente del exterior de la entidad, de esta manera ganaríamos en independencia y objetividad, pero deben ser conocedores de los sistemas que empleamos y es preferible, si no necesario, que tengan una experiencia afín y conocimientos del sector.

Por el contrario, si contratamos personal proveniente de la propia entidad tendríamos ventajas en cuanto a garantías, ya que son personas conocidas y conocen el entorno, se sabe su formación y cuánto saben de las distintas áreas de informática, así como su trayectoria.

b) Auditoría informática externa

Es la que realiza una entidad no vinculada de ninguna manera a la entidad auditada, especializada en el servicio que se contrata. Obviamente, este tipo de auditoría informática permite garantizar una gran objetividad e independencia. Algunos factores a tenerse en cuenta son los siguientes.

i) Cómo seleccionar la empresa auditora
Deben considerarse varias entidades que cumplan con las condiciones que se fijen y seleccionar la mejor opción, y nunca decantarse por la entidad recomendada directamente por el director de informática.

ii) Quien decide la entidad
Para seleccionar la entidad auditora se deberá tener en cuenta principalmente el objetivo de la auditoría.

iii) Cómo contratar
Debe realizarse una contratación formal que especifique el objetivo, el alcance del proceso de auditoría, el ámbito geográfico, las características del proceso a realizar, los resultados a obtener y tanto el marco temporal como el económico.

iv) Plan de trabajo previo
Es recomendable que exista un plan de trabajo a realizar, sin que por ello se evite el factor sorpresa.

v) Cláusulas especiales
Aunque debe sobreentenderse, es necesario especificar cláusulas de confidencialidad, así como el compromiso por parte de la entidad auditora a cumplir todas las normas internas del cliente y especialmente las referidas a seguridad.

c) Relación entre auditoría interna y auditoría externa

Una vez vistos los dos tipos de auditorías informáticas que existen, debemos comentar algunos factores referentes a la relación entre ambos.

i) Compatibilidad
Tanto la auditoría informática interna como la externa son totalmente compatibles y recomendables, ya que tienen un cometido complementario.

ii) Colaboración
Los externos deben apoyarse en el trabajo de los internos, pero siempre sin perder objetividad ni independencia. Los internos deben figurar entre los interlocutores de los externos, si bien éstos han de reflejar en sus informes, si fuera necesario, hechos o deficiencias achacables a los internos.

iii) Formación
Los externos pueden aportar técnicas y métodos, por su gran experiencia, a los internos.

iv) Creación
La auditoría interna puede crearse por recomendación de la externa.

3.3 - El auditor informático

Por la gran responsabilidad que se lo otorga al auditor, parece obvio que debe cumplir una serie de requisitos que garanticen su buen hacer en su trabajo. Vamos a ver el **perfil** que se le desea un buen auditor informático, así quienes **componen un grupo de auditoría informática** y cuales son las **funciones** de cada uno y las **relaciones** que éstos tendrán con otros profesionales.

3.3.1 - El perfil del auditor informático

En cada caso habrá que definir el perfil específico, pero en principio el auditor informático habrá de tener un nivel suficiente de las cualidades y requisitos que se muestran a continuación.

i) Formación
La formación deberá incluir aspectos técnicos de sistemas y tecnologías de la información, así como de auditoría y de control, más aspectos complementarios sobre cómo elaborar y manejar cuestionarios, cómo realizar entrevistas y cómo redactar informes.

ii) Experiencia
La experiencia deberá estar relacionada con la tecnología, puestos clave de las diferentes áreas. Es deseable, además, el conocimiento del sector. Si no se tienen la formación y experiencia necesarias, la auditoría informática no tendrá el nivel necesario, y al tratarse en definitiva de un “duelo” entre auditores y auditados, el auditado, quienes se defienden para recibir un informe benigno, podrán llevar al auditor al terreno que más le convenga.

iii) Independencia
La independencia le supone al auditor una actitud mental que le permite actuar con libertad con respecto a su juicio profesional, para lo cual debe encontrarse libre de cualquier predisposición que limite su imparcialidad en la consideración objetiva de los hechos, así como en la formulación de sus conclusiones. Esto les permite actuar desde un punto de vista imparcial.

iv) Objetividad
La objetividad implica el mantenimiento de una actitud imparcial en todas las funciones del auditor. Para ello deberá gozar de total independencia en sus relaciones con la entidad auditada. Debe ser justo y no permitir ningún tipo de influencia o perjuicio.

v) Madurez
La madurez está muy relacionada con la formación y la experiencia, e implica que el auditor tenga buen juicio y sensatez.

vi) Integridad
La integridad debe entenderse como la rectitud intachable en el ejercicio profesional, que le obliga a ser honesto y sincero en la realización de su trabajo y en la emisión del informe. Esto implica que el auditor adopte una honradez en su trabajo irreprochable.

vii) Capacidad de análisis y síntesis
Dado que la elaboración de una auditoría conlleva la realización de muy diversas fases, el auditor debe tener una capacidad de análisis y de síntesis que le otorgue una gran capacidad de abstracción.

viii) Seguridad en sí mismo
El auditor debe tener los conocimientos y experiencia suficiente como para tener una gran seguridad en sí mismo, para demostrar así a la entidad auditada que se está realizando un trabajo de calidad y con propiedad.

ix) Responsabilidad
Como ya hemos comentado anteriormente, la elaboración de una auditoría supone una gran responsabilidad para los auditores, puesto que la entidad auditada deposita en nosotros la confianza para encontrar todos los posibles fallos o anomalías, de manera que puedan ser así corregidos. De existir y no encontrarse podríamos hacer que la entidad auditada sufra las consecuencias.

x) Interés
La elaboración de una auditoría es una labor que requiere un gran esfuerzo, y por conllevar una gran responsabilidad, es necesario que el auditor tenga un gran interés por el buen hacer de ésta.

xi) Puesta al día de los conocimientos
Como hemos comentado, la formación es muy importante y el primer aspecto a tener en cuenta en un auditor, por tanto deberá estar al tanto de todas las posibles novedades que puedan ir surgiendo en los campos de actuación del auditor. De todos los conocimientos que debe tener, los técnicos son los más cambiantes.

xii) Perfil y conocimientos específicos
Lógicamente, hemos dado un perfil general que debe tener un auditor. Éste dependerá y será específico dependiendo de los siguientes aspectos.

xii.i) Nivel del puesto que ocupe en la labor de auditoría. Veremos a continuación los distintos niveles que existen.

xii.ii) Entorno de trabajo del auditor.

xii.iii) Áreas a auditar. Es la parte más técnica. Las áreas pueden ser seguridad, desarrollo, calidad, gestión, etc.

3.3.2 - Funciones generales

Aunque, como veremos a continuación, dependiendo del puesto que ocupe dentro del equipo humano, cada auditor tendrá unas funciones concretas. Existe un **código ético de ISACA** donde se muestran las funciones generales de los auditores, necesario en todas las funciones y fundamental para la auditoría informática. Vamos a ver un resumen.

i) Estándares, procedimientos y controles
Fomentar el establecimiento y equipamiento de estándares, procedimientos y controles adecuados, en los sistemas de información. Cumplir con los estándares de auditoría de los sistemas de información que han sido adoptados por la ISACF (Fundación de la ISACA).

ii) Lealtad y honradez
Servir con diligencia, lealtad y honradez los intereses de empleados, accionistas, clientes y público en general. No participarán conscientemente en ninguna actividad ilegal o impropia.

iii) Confidencialidad, objetividad e independencia
Garantizar la confidencialidad de la información obtenida en el ejercicio de sus funciones. No usarán dicha información en beneficio propio, ni dejarán que llegue a terceros o no pertinentes. Cumplir sus funciones de forma objetiva e independiente, evitando actividades que pongan en entredicho, o lo parezca, su independencia.

iv) Estar al día en auditoría informática
Mantener su competencia en los campos interrelacionados de la auditoría informática y los sistemas de información, mediante su participación en las actividades de desarrollo profesional.

v) Procurar pruebas objetivas suficientes
Aplicar el debido cuidado para obtener y documentar pruebas objetivas suficientes, en que basar sus conclusiones y recomendaciones.

vi) Informar a los interesados
Informar a las partes interesadas sobre los resultados del trabajo de auditoría efectuado.

vii) Fomentar la formación e información

Fomentar la formación de directivos, clientes y público en general, para que mejore su entendimiento de lo que son la auditoría informática y los sistemas de información.

viii) Altos estándares de conducta
Mantener altos estándares de conducta y comportamiento personal en sus actividades, tanto profesionales como privadas.

3.3.3 - El equipo humano

El quipo humano está compuesto por una o más personas, aunque lo normal es que exista un equipo de trabajo formado por varias personas. Puesto que se trata de un equipo, han de actuar como tal y no individualmente, sobre todo porque lo que se haga lo tienen que entender los demás, previendo sustituciones, enfermedades y continuidad para otras revisiones en el futuro, entre otros factores. Aunque la organización de los equipos y el número de personas dependerá de la experiencia de sus componentes y del entorno, vamos a ver quienes integran generalmente un equipo de trabajo.

a) Gerente

Es posible que se designen varios y sus funciones serán las que se determinen en cada entidad, y con aspectos diferenciales si se trata de auditores externos o internos. Vamos a indicar las funciones más generales.

i) Planificación del trabajo
La planificación del trabajo determinará qué hacer y cuándo se debe hacer. Debe ser aprobada por un nivel superior.

ii) Definición de los objetivos
Para saber qué hacer se deben definir los objetivos de la auditoría informática. Éstos dependerán de cada caso en concreto.

iii) Elaboración del programa de trabajo
Sería similar a la planificación del trabajo, pero de una manera más concreta.

iv) Dirección del proyecto de auditoría
En general, es el director del proyecto en concreto. Tomará las decisiones oportunas sobre la marcha y definirá las pautas a seguir y los posibles cambios.

v) Revisión del informe
La revisión de los informes realizados por su grupo de trabajo o por otros gerentes tiene la ventaja de la experiencia acumulada y la independencia que aporta otra persona.

vi) Seguimiento de las recomendaciones
Sólo en el caso de los auditores informáticos internos, ya que normalmente la función de los externos finaliza con la entrega del informe, especialmente cuando existe la función interna.

b) Jefe de equipo

Puede determinarse que haya varios, dependiendo de las circunstancias de la entidad en concreto y sus funciones serán distintas si son internos o externos. Vamos a ver las más generales en ambos casos.

i) Colaboración con el gerente
Deben colaborar con todas las funciones que debe llevar a cabo el gerente.

ii) Supervisión del trabajo de campo
Serán los encargados de supervisar el trabajo de campo que se realice, así como colaborar en la medida de lo posible en la realización de éste.

iii) Coordinación y revisión del trabajo de los auditores
En general, deberán determinar las funciones en concreto que deben realizar los auditores, así como coordinarlas y supervisarlas.

iv) Detección de los puntos importantes para informe
Deben conocer cuales son los aspectos, situaciones o circunstancias a tener en cuenta para el desarrollo del informe, como debilidades, errores, consideraciones, etc.

v) Propuesta de recomendaciones
De la misma manera, deben proponer las recomendaciones a seguir por la entidad auditada para solventar las deficiencias que se pudieran en encontrar.

vi) Elaboración del borrador del informe
Son los encargados de elaborar el borrador del informe que se le entregará a la entidad auditada, con las deficiencias, errores o debilidades encontradas y las recomendaciones propuestas.

c) Los auditores

Los auditores, generalmente varios, van a ser los que realicen el trabajo propuesto y coordinado por los gerentes y jefes de grupo. Vamos a ver sus funciones más importantes.

i) Colaboración con los jefes de grupo
Como veremos a continuación, sus funciones implican colaborar de cerca con los jefes de grupo.

ii) Realización del trabajo de campo
Como veremos más adelante, el trabajo de campo es el trabajo que se realiza en la entidad auditada, como puedan ser entrevistas al personal, pruebas y verificaciones, análisis de la documentación o la gestión de los papeles de trabajo.

iii) Propuesta de sugerencias
Puesto que van a ser los primeros en toparse con los posibles errores o deficiencias, y dado que van a analizar en primera persona los equipos o sistemas informáticos,

deberán proponer a los jefes de grupo realizar verificaciones complementarias o aspectos a tener en cuenta, tanto en cuando lo crean conveniete.

iv) Propuesta de recomendaciones
Como expertos del campo a tratar que son, deben proponer las sugerencias a los jefes de grupo para las recomendaciones finales.

d) Auditores *junior*

Los auditores *junior* son aquellos que están empezando a realizar auditorías, y que por tanto carecen de la experiencia necesaria. En un equipo de trabajo no tiene porqué haber auditores *junior*, pero si la entidad auditora dispone de éstos, deberán formar parte de los equipos para conseguir alcanzar los valores necesarios de experiencia, madurez y formación y así poder llegar a ser auditores.

Por tanto, si se integran en el equipo auditores *junior*, hay que considerar que su aportación inicial no será importante y que al principio más que ayudar se formarán.

3.4 - Realización de la auditoría informática

En la realización de cualquier auditoría informática podemos diferenciar tres grandes fases: **trabajo preparatorio**, **trabajo de campo** y **desarrollo del informe**. Vamos a ver cada una de ellas en profundidad.

3.4.1 - Trabajo preparatorio

Es la primera fase que se realiza en la auditoría informática y es cuando vamos a analizar los requisitos y necesidades de la entidad a auditar para así poder planificar nuestro plan de actuación. Vamos a ver los distintos aspectos que debemos cubrir en esta fase.

a) Encargo del proyecto

El encargo puede corresponder a un trabajo puntual que haya surgido en relación con un problema de la entidad o por el contrario, corresponder a un trabajo que estaba previsto en el **plan de auditoría** de la entidad y que ha llegado el momento de abordar. En cualquiera de los dos casos, antes de aceptar la realización del proyecto, especialmente si se trata de una auditoría externa, se debe estar totalmente seguro de que se cuentan con los medios y personal cualificado suficientes para realizar el trabajo con las máximas garantías. Por tanto, antes de aceptar el trabajo se deberá hacer un pequeño análisis del objetivo, ámbito y alcance del mismo.

Una vez que se ha aceptado la realización de la auditoría, se debe realizar la 7planificación de la misma, para así poder concretar el objetivo, el ámbito, el marco temporal y económico y la profundidad, entre otros factores, que deben quedar plasmados en un **contrato formal**.

b) Planificación

Estos factores deben quedar bien definidos antes de comenzar el proceso de auditoría informática, ya que van a definir la organización y la manera de actuación durante la misma.

i) Responsables
Para realizar la planificación, es importante que la entidad auditada designe a un coordinador único del proyecto, tanto si la auditoría es interna como si es externa, que será con quien se acordarán las actividades a desarrollar, así como las acciones que debe realizar la entidad auditada para que la auditoría se pueda realizar rápida y eficazmente. Por parte de la entidad auditora, si ésta es externa, se debe designar a un responsable del proyecto, que será un socio de esta entidad.

ii) Código del proyecto
Se debe asignar un código al proyecto según la normativa de la entidad, de esta manera podremos identificarlo de manera inequívoca.

iii) Análisis de objetivos
Como ya hemos comentado, los objetivos a cubrir por la auditoría van a determinar el desarrollo de la misma, así como encaminar los resultados a estos propósitos concretos. En definitiva, son el motivo de la auditoría. Excepcionalmente pueden existir otros objetivos y los auditores sólo conocer los secundarios. Por ejemplo, el objetivo de la auditoría puede ser conocer las deficiencias en cuanto a Seguridad Física de los sistemas de información, para tomar la entidad auditada una decisión sobre su responsable.

iv) Profundidad
Otro factor importante y que debe quedar perfectamente claro antes de comenzar la auditoría informática es la profundidad de la misma, ya que puede ser desde una revisión general de algunos sistemas hasta un análisis exhaustivo de ciertos procesos, departamentos o formas de gestión. En la planificación se debe concretar la profundidad de la auditoría, hasta donde se deben analizar los objetivos, el nivel investigación que se va a adoptar, el tamaño de las muestras que se van a tomar, el número de entrevistas y pruebas, etc.

v) Ámbito
Con ámbito nos referimos a las zonas de actuación de la auditoría. Ha de quedar también perfectamente definido, especialmente en entidades grandes y dispersas, por lo que se especificarán las tareas por centro, así como las zonas geográficas de actuación.

vi) Marco temporal
El marco temporal en el que se va a realizar la auditoría debe quedar definido en la planificación. Éste dependerá de los objetivos, el alcance y la profundidad de la auditoría, dependiendo de estos factores, así se asignarán tiempos.

vii) Marco económico
El marco económico de la auditoría se refiere al coste que va a suponer la realización de la misma para le empresa auditada. En el caso de que la auditoría sea interna, se tendrán

unos gastos de personal, medios, investigación, etc. En el caso de que sea externa, a los costes de la auditoría hay que añadir los honorarios de la empresa auditora. En cualquier caso, los costes van a depender de los objetivos, alcance, profundidad, ámbito y duración de la auditoría, así como de los recursos técnicos y la logística necesarios para llevarla a cabo.

viii) Equipo de auditores
Dependiendo de los factores que hemos ido viendo, se deberá crear el equipo de auditores, que será quienes lleven a cabo el proyecto. Es posible que se incluyan expertos en determinados campos para poder auditar sistemas concretos. Una vez definido el equipo, es necesario que se reúna para explicar los objetivos y asegurarse de que todos los integrantes coinciden en la interpretación del proyecto.

ix) Recursos técnicos
Se debe analizar cuáles van a ser los recursos técnicos necesarios para llevar a cabo la auditoría. Lógicamente, éstos dependerán de cada caso en concreto e influirán en el coste de la misma. Con recursos técnicos nos referimos a equipos de auditores, herramientas necesarias, sistemas de comunicaciones que se van a emplear, adaptación o realización de cuestionarios y pruebas, etc.

x) Logística
Con la logística nos referimos al transporte y alojamiento de los auditores, el acceso a las instalaciones, si dispondrán de despacho en la entidad a auditar, etc. Generalmente es un aspecto a tener muy en cuenta si se trata de auditorías externas, pero puede darse el caso que en la realización de una auditoría interna, los auditores tengan que desplazarse a otros edificios, incluso a otras ciudades o países, por lo que este punto tendrá que quedar bien claro.

c) Programa de trabajo

En el programa de trabajo se especificará de una manera mucho más concreta la forma de cubrir los objetivos mediante la definición de las tareas. Se debe concretar quién las va a realizar, las fechas para cada una de ellas, cómo se realizarán, medios necesarios, etc. Cuando se especifique el programa de trabajo, es necesario que se notifique a los departamentos o áreas implicadas en la auditoría que van a ser auditadas, sin eliminar el posible factor sorpresa.

3.4.2 - Trabajo de campo

El trabajo de campo es la realización de la auditoría en sí. Ajustándose a lo desarrollado en la planificación y más concretamente en el plan de trabajo, se va a realizar la **recopilación de información** para después analizarla y obtener las evidencias suficientes que nos permitan elaborar un informe.

La recopilación de la información es el trabajo que vamos a realizar en la entidad auditada. Existen diferentes métodos y técnicas dependiendo de las fuentes para recopilar la información necesaria y poder elaborar el informe, que es el fin de la auditoría. Las distintas fuentes de donde podemos obtener información son

documentación, **personal**, **revisiones y pruebas** y **fuentes externas a la entidad**. Vamos a ver las de carácter más general, puesto que en función de los objetivos de la auditoría se seleccionarán las fuentes más idóneas.

Es importante recordar que los auditores mantendrán **confidencialidad** sobre la información que reciban o conozcan, que puede referirse a remuneraciones, clientes, datos personales, vulnerabilidades de la entidad, etc. y especialmente respecto a aquellas informaciones que en la entidad estén clasificadas como confidenciales o restringidas.

a) Documentación

La documentación ya existente en la entidad es una gran fuente de información sobre ésta, por tanto se tendrá que recopilar y analizar. Es importante concretar, y si se trata de auditoría externa, incluso recoger en un contrato formal, el nivel de confidencialidad de estos documentos y si se podrán fotocopiar, sacar de la entidad, etc. Vamos a ver los más representativos.

i) Políticas, estándares y procedimientos
Se deben analizar las políticas, estándares y procedimientos que se emplean para el desarrollo de la y producción informático de la entidad, así como para su gestión y seguridad. Aún en la actualidad existen entidades que no aplican políticas o estándares, por lo que una recomendación a incluir en el informe final será la creación y aprobación de éstos.

ii) Planes informáticos
Los planes son necesarios para verificar que la informática de la entidad está bien orientada y tiene un rumbo fijo.

iii) Organigramas
Se deben analizar los organigramas existentes en la entidad, para entender las áreas principales que existan y verificar su situación, nivel y dependencia de informática.

iv) Presupuestos y seguimientos
Es importante analizar los presupuestos relacionados con la informática, para así ver los rangos económicos en los que nos movemos y así verificar que los presupuestos se ajustan los dispositivos y sistemas disponibles.

v) Informes anteriores
Si existen informes anteriores de otras auditorías informáticas, ya sean internas o externas, se deberán solicitar para analizarlos y así estar al corriente de la situación previa de la entidad.

vi) Actas de reuniones relacionadas
Se deben solicitar las actas de las reuniones relacionadas con los sistemas informáticos, ya que son una gran fuente de información.

vii) Informes de suministradores y consultores

Los suministradores y consultores que proporcionen soluciones concretas a la entidad auditada deben desarrollar una serie de informes, de los cuales obtendremos una gran cantidad de información.

viii) Memorandos, circulares y comunicados
De esta manera podremos conocer cual es la información al respecto que se les da a los usuarios en general, si es adecuada y si se cumple.

ix) Planos, contratos y pólizas de seguros
Los planos de las instalaciones nos van a proporcionar una gran cantidad de información técnica a cerca de éstas. Los contratos son importantes para conocer, sobre todo, las cláusulas que debieran existir. En cuanto a las pólizas de seguros, nos proporcionarán información acerca del gasto destinado a la aseguración de bienes, los elementos o dispositivos protegidos y ante qué circunstancias, etc.

x) Otros documentos
Es posible encontrar una gran cantidad de información acerca de la entidad en otros documentos, como su página Web, foros en Internet, si se trata de una gran compañía, memorias de la entidad, etc.

b) Personal

Obviamente, una gran fuente de información acerca de la entidad son sus empleados, por este motivo es necesario que la auditoría cuente éstos para recabar información. Las dos maneras más usuales para ello son mediante **cuestionarios** o mediante una **entrevista personal**. Ambos métodos son necesarios y complementarios.

Un factor a tener en cuenta es el de **muestreo estadístico**, tanto para las entrevistas, como para los cuestionarios. Con ello se evita "analizar" el cien por cien de las posibles fuentes, en este caso, del personal de la entidad, ya que en muchos casos no es rentable o, incluso, factible. Para ello se debe escoger una muestra del total que será la que se analizará. Esta muestra debe ser representativa y significativa, para que los resultados que obtengamos sean los más parecidos al los que hubiéramos obtenido analizando al cien por cien de las fuentes. Lógicamente, cuanto más cerca esté el porcentaje analizado del cien por cien, más fiable será el muestreo, por lo que se debe encontrar el punto de equilibrio en el que, con un coste mínimo, se tenga una fiabilidad suficiente. En función del análisis del muestreo el auditor decidirá si se debe analizar una muestra más amplia o considera que el resultado es satisfactorio. Para la tabulación y cálculo de resultados se suelen emplear paquetes estadísticos, generalmente, informáticos.

i) El cuestionario

El cuestionario es una batería de cuestiones que el auditor entrega al auditado para que éste las conteste. El cuestionario puede estar en cualquier formato, aunque lo más común es que es que estén en papel o bajo soporte informático. En cualquier caso, existen unas **consideraciones generales** que se deben tener en cuenta en cada caso y el **tipo de cuestionario** que vamos a emplear. Como veremos más adelante, es necesario que se verifique la información recabada en los cuestionarios.

i.i) Consideraciones generales

A la hora de preparar y desarrollar el cuestionario se deben tener presentes los siguientes aspectos.

i.i.i) Útil y válido
El cuestionario es válido y necesario en la auditoría informática, por lo que es una herramienta principal en el desarrollo de cualquier auditoría.

i.i.ii) Entendido por el auditor
Es fundamental que el propio auditor entienda perfectamente las preguntas todo su alcance, ya que si el auditado pide aclaraciones y el auditor no es capaz de darle una respuesta razonable, el efecto es muy negativo, y al final se dudará incluso de la validez del informe, del diagnóstico y de las posibles recomendaciones. Por tanto, el auditor debe haber analizado el cuestionario y consultado los puntos que le puedan quedar más oscuros.

i.i.iii) Auditor sin experiencia
El disponer de un buen cuestionario no hace que los auditores sin experiencia realicen su trabajo como expertos, pero los cuestionarios ayudan a recordar todos los puntos a verificar.

i.i.iv) Incluir aclaraciones
Especialmente si está en soporte informático, se deben incluir aclaraciones, explicaciones, incluso, ayudas en línea, acerca de las preguntas y del propio cuestionario.

i.i.v) Contradicciones
Un factor muy importante es que no existan contradicciones, tanto en el propio cuestionario como entre éste otras pruebas o análisis realizados en la auditoría.

i.i.vi) Preguntas concretas
Las preguntas deben ser concretas, sin dejar lugar a ambigüedades que puedan llevar a confusión y por tanto, unos resultados que no se ajusten a la realidad. Además, es importante que la forma en que estén redactadas las preguntas no conduzca a las respuestas.

i.i.vii) Evitar jergas
Se debe evitar el uso de jergas y tecnicismos que puedan resultar difíciles de comprender para los auditados.

i.i.viii) Estructuración
El formulario debe estar bien construido, agrupando las preguntas por temas para facilitar su realización.

i.i.ix) No cuestiones irreales
Entendemos por cuestiones irreales todas aquellas en las que podemos saber las respuestas más probables. Un ejemplo claro es preguntar sobre el sueldo, de los

empleados, ya que lo más probable es que un gran porcentaje de los auditados respondan que es bajo.

i.i.x) Adaptar las cuestiones
Se podrá disponer de cuestionarios generales que se deben adaptar para cada entidad y auditoría en concreto, dependiendo del objetivo y la profundidad de ésta, además de otros factores más concretos, como el entorno, la dependencia de la informática, las características de la entidad, etc.

i.i.xi) Importancia de cada punto
La posible importancia de cada punto es algo muy complejo, que dependerá en todo caso de otros factores, como el entorno. No obstante, pueden incluirse unos índices de pesos que determinen la importancia de cada punto.

i.i.xii) Auditor presente
El auditor puede estar presente o no cuando el auditado realice el cuestionario. En cualquier caso, se debe informar de la opción que se va a escoger. Si está presente el auditor podrá resolver dudas que puedan surgir, pero es posible que condicione de alguna manera las respuestas.

i.i.xiii) Datos
Se debe barajar la opción de incluir en el cuestionario los datos del auditor, del auditado y de las circunstancias en las que se ha realizado, como fecha y hora, lugar de realización e incluso, observaciones generales.

i.ii) Tipos de cuestionarios

Como ya hemos comentado, al margen del formato en el que se realice el cuestionario, existen varios tipos, en función del tipo de preguntas y, consecuentemente, de respuestas. Vamos a ver los más comunes.

i.ii.i) Simples
Las respuestas pueden ser SÍ, NO y N/A. Son útiles cuando las respuestas no requieren cuantificación. Si hicieran falta explicaciones u observaciones adicionales se pueden incluir espacios habilitados para ello.

i.ii.ii) Cuantificables
Las respuestas toman un valor numérico dentro de un rango establecido. Lo normal es de 0 a 5 o de 0 a 10. Debe quedar perfectamente definido cuál es significado de cada número en cada pregunta en concreto.

i.ii.iii) Matrices
No se suelen emplear para que los contesten los auditados, si no más bien para recopilar información por parte de los auditados en sus verificaciones y análisis. Pueden adoptar múltiples formatos, por lo que su uso y formato queda muy abierto.

ii) La entrevista

La entrevista es un diálogo entre el auditor y auditado para recabar información. Aporta datos y pistas que no se obtienen por otros medios. Excepcionalmente, puede haber varios entrevistados a la vez, pero les impedirá hablar con claridad y les permitirá "arroparse". Otra posible situación es que haya más de un auditor para reforzar, lo que puede aturdir al entrevistado y darle más sensación de interrogatorio, pero facilita y enriquece el trabajo. Esto suele ser normal cuando uno de los auditores no tiene experiencia y, normalmente, se limita a tomar notas. En cualquier caso, de existir más de un auditor, deben estar totalmente compenetrados para no contradecirse.

Para la realización de la entrevista, se requiere una planificación y preparación previa. Vamos a ver a continuación los puntos que se deben abordar en el **trabajo previo**, así como **cómo se debe desarrollar la entrevista**, **qué es lo que no se debe hacer** y el **trabajo posterior a la entrevista** que se debe realizar. Al igual que en los cuestionarios, se debe hacer una selección de a quién se va a entrevistar. Se puede realizar un muestreo estadístico o seleccionar al personal que nos interese en cada caso en concreto, por ser la entrevista algo más personal. Además, es necesario que después de realizar la entrevista, se verifiquen tantos datos como sea posible.

ii.i) Preparación de la entrevista

Para realizar una entrevista que nos aporte la información suficiente y que resulte lo más cómoda para el entrevistado y productiva para el entrevistador, se debe realizar una labor de preparación previa. Vamos a ver los aspectos más importantes de ésta labor.

ii.i.i) Propósito
Es muy importante que la entrevista se prepare para obtener unos datos determinados, por tanto, se debe analizar el propósito de la entrevista y tenerlo muy claro, para que con las preguntas que realicemos obtengamos la información que deseamos.

ii.i.ii) Revisar la información disponible
Se debe analizar si la información a averiguar no la hemos obtenido ya por otros medios o la podríamos obtener de otra manera más sencilla, con esto evitaremos obtener información ya disponible o molestar al entrevistado. A no ser que lo que intentemos sea contrastar opiniones o disponer del testimonio o confirmación del entrevistado. Aún así, es conveniente entrevistar a varias personas de una misma función para contrastar.

ii.i.iii) Temas clave
Debemos identificar cuáles serán los temas clave de la entrevista, de esta manera podremos obtener información concreta y precisa sobre éstos, dejando los menos importantes de lado.

ii.i.iv) Preparar las preguntas
Al igual que sucedía con los cuestionarios, es posible que el personal auditor tenga preparadas unas baterías de preguntas estándar o generales. Éstas se deben adaptar para cada auditoría, e incluso para cada persona y entrevista en concreto.

ii.i.v) Seleccionar las funciones

Es importante que el entrevistador esté a la altura de la situación, por ello si se va a realizar una entrevista a altos cargos, directivos o personal experto, el auditor deberá tener un nivel y experiencia adecuados.

ii.i.vi) Seleccionar las personas
Como ya hemos comentado, aunque no es lo normal, es posible que se entrevisten a varias personas a la vez, lo que habrá que planificarse y valorar. Algo más común es que la entrevista la realicen varias personas, en este caso se tendrán que poner de acuerdo en los temas a tratar y la preparación la tendrán que realizar conjuntamente.

ii.i.vii) Fecha y hora
El momento más conveniente para realizar la entrevista es a media mañana, cuando el entrevistado a tenido tiempo de resolver los asuntos más urgentes del día. Se debe evitar la primera y última hora, así como realizar la entrevista inmediatamente después de las comidas.

ii.i.viii) Lugar
Si el despacho o puesto de trabajo del entrevistado no permite la confidencialidad y tranquilidad necesarias o se producen interrupciones continuas, es preferible utilizar una sala de reuniones o despacho aislado e idóneo.

ii.i.ix) Suministrar información
Suele ser conveniente enviar con antelación una carta o nota a la persona a entrevistar, así como a alguno de sus supervisores, informando del motivo y particularidades de la entrevista e incluso, de los puntos que se van a tratar. Esto facilitará el trabajo, pero puede suponer la pérdida del factor sorpresa, que en algunos casos es imprescindible. Por ejemplo, un plan de contingencia no se puede improvisar de un día para otro, pero si se quiere verificar la existencia de copias de seguridad, adecuadas y recientes, es mejor no avisar, porque sí es algo que se pueda improvisar o disimular en pocas horas.

ii.ii) Realización de la entrevista

Vamos a ver a continuación las pautas generales de cómo se debe realizar la entrevista a fin de obtener la máxima productividad de la misma y hacer que el entrevistado se sienta lo más cómodo posible.

ii.ii.i) Introducción y presentación
En la introducción hay que intentar tranquilizar al entrevistado, ya que en ocasiones su tensión impide el desarrollo de la entrevista, sin quitarle ni importancia ni rigor al proceso. A veces en conveniente comentar que la auditoría tiene similitudes con una revisión médica.

ii.ii.ii) Comentar el tiempo que se va a invertir
Es importante que el entrevistado conozca el tiempo que va a durar la entrevista. Ésta no deberá sobrepasar una la hora de duración.

ii.ii.iii) Crear y mantener el ambiente adecuado
Para el buen desarrollo de la entrevista, es necesario que el auditor sepa crear y mantener el ambiente adecuado.

ii.ii.iv) No grabar
No se debe grabar la conversación, ya que ello es muy probable que ponga nervioso al entrevistado, por darle la sensación de interrogatorio.

ii.ii.v) Tomar notas
Para poder analizar toda la información que se recopila, es necesario que el entrevistador tome notas. Es conveniente que se le explica al entrevistado esta necesidad. No deben tomarse demasiadas notas, si no escribir lo fundamental, incluso con abreviaturas. Para ello se pueden tener las preguntas preparadas de forma que baste con anotar una o varias respuestas, tomar porcentajes, etc.

ii.ii.vi) Empezar por preguntas sin tensión
Puesto que existen preguntas que conllevan más tensión que otras, es conveniente que el auditor empiece por las preguntas más suaves, para que el entrevistado se adapte a la situación lo más cómodamente posible.

ii.ii.vii) Saber escuchar
El entrevistador tiene que tener la capacidad para que el entrevistado pueda comentar tranquilamente toda la información que se le solicita, para ello tiene que saber escuchar cuando el otro está hablando.

ii.ii.viii) Conocimientos técnicos
Es imprescindible que el entrevistador tenga los conocimientos técnicos suficientes para entender todo lo que le dicen, y evitar así que el entrevistado le lleve al terreno que más le convenga.

ii.ii.ix) Satisfacer dudas
Es posible que al entrevistado le puedan surgir dudas razonables, sobre todo si no se le ha informado antes de la entrevista o si se trata de las primeras entrevistas en un proceso de auditoría. El auditor debe satisfacer todas estas dudas, las más comunes son el motivo de la entrevista, porqué ha sido seleccionado, cómo se usarán sus respuestas o la finalidad de la auditoria, que puede ser conveniente comentar, salvo que como auditores no podamos dar ningún tipo de explicación.

ii.ii.x) Detectar indicios no verbales
Existen ciertas reacciones por parte del entrevistado, como gestos, sofocos, cambios de postura, etc. que el auditor debe ser capaz de detectar e interpretar, ya que pueden aportar información extra.

ii.ii.xi) Escuchar entre líneas
A veces los auditados quieren dar a entender algo que no se atreven a manifestar abiertamente. Esos mensajes hay que saber captarlos y tratar de interpretarlos y contrastarlos.

ii.ii.xii) Puertas abiertas
Al finalizar la entrevista se le deben dejar al entrevistado las puertas abiertas para futuras entrevistas o para que en un momento dado amplíe el entrevistado la información que nos ha facilitado.

ii.iii) Qué evitar

Existen ciertos factores o situaciones que el auditor debe evitar en la realización de la entrevista. Es importante que éste tenga la capacidad para hacerlo, ya que es probable que el entrevistado cree o promueve estas situaciones.

ii.iii.i) Orientar la respuesta
El auditor no debe anticipar las respuestas ni inducir en sus preguntas a una respuesta determinada.

ii.iii.ii) Crear tensión o agresividad
Para el buen desarrollo de la entrevista, es necesario que no se cree tensión ni agresividad, realizando determinadas preguntas, con determinado tono, mirada, gestos, etc.

ii.iii.iii) Interrogar
La entrevista debe ser fluida y natural, sin dar la sensación de interrogatorio.

ii.iii.iv) Acusar
El auditor no debe dar la sensación de que está acusando de nada al entrevistado o de que está sometiéndolo a una serie de preguntas buscando que falle en algo, como si fuera su único cometido en la auditoría.

ii.iii.v) Criticar o discutir
El auditor no debe criticar ni dar su opinión sobre los aspectos que se comenten, debe ser objetivo y limitarse a realizar las preguntas y analizar las respuestas.

ii.iii.vi) Uso de jergas
Se debe evitar el uso de jergas y tecnicismos que puedan resultar desconocidos para el entrevistado. Por otro lado, es probable que aparezcan expresiones técnicas propias de un fabricante, equipo o paquete en exclusiva, o incluso, expresiones que se usan en una sola instalación. En cualquier caso, si sale algún término desconocido deberemos preguntar y pedir que nos explique su significado.

ii.iii.vii) Intercambio de roles
No hay que intercambiar los roles, lo que ocurre a veces cuando el auditor asume el papel del auditado, sobre todo cuando el auditor ha sido previamente informático y asocia situaciones con otras vividas por él. También puede ocurrir cuando el auditado se considera más preparado que el auditor o ha asistido a seminarios o leído publicaciones especializadas.

ii.iii.viii) Dar consejos
El auditor no debe dar consejos, ya que pueden volverse contra él después. Debe dejar bien claro que las únicas opiniones y recomendaciones válidas por su parte son las contenidas en el infirme oficial.

ii.iii.ix) Dar sensación de prisa

Para que el entrevistado pueda comentarnos tranquilamente todo lo que tiene que decir, y así poder recopilar toda la información posible, no tenemos que darle la sensación de prisa.

ii.iv) Trabajo posterior a la entrevista

Una vez que se ha realizado la entrevista, es necesario que se realicen unas tareas para organizar la información obtenida y así poder emplearla para el desarrollo del informe. Las tareas que mostramos a continuación se deben realizar lo antes posible, ya que el auditor recordará con más precisión las ideas y conceptos tratados en la entrevista.

ii.iv.i) Revisar y analizar notas
Se deben analizar y revisar las notas que hemos tomado durante la entrevista, ampliándolas cuando se crea oportuno y organizándolas para facilitar su uso.

ii.iv.ii) Pasar las notas a limpio
Una vez que hemos analizado, revisado y comentado las notas que hemos obtenido, se deben pasar a limpio, estructurando y concretando la información obtenida en la entrevista. Además es imprescindible que separemos los hechos de los comentarios y opiniones personales.

c) Revisiones y pruebas

Posiblemente la manera de obtener la información más fiable es mediante la observación, revisión y pruebas *in situ* de las áreas, campos o dispositivos a auditar. Lógicamente, éstos dependerán en gran medida de los objetivos y la finalidad de la auditoría. Mediante las revisiones y pruebas podemos además corroborar la información que hemos obtenido anteriormente con la documentación, cuestionarios o entrevistas, así como rebatir afirmaciones. Es posible que se presente documentación que acredite que se cumple con la normativa y que las respuestas obtenidas en las entrevistas lo corroboren, pero debemos conocer la realidad de forma directa mediante este tipo de análisis.

Como hemos comentado, las pruebas y revisiones dependerán en gran medida de la finalidad de la auditoría, por tanto las técnicas y métodos que se empleen serán muy diferentes y concretos para cada caso. Por este motivo se sale del alcance de este trabajo el analizar todas y cada una las técnicas existentes para revisar los posibles sistemas a auditar. Si bien podemos mencionar que existen unas técnicas y estándares para analizar los distintos sistemas, dejamos este punto muy abierto a decisión de los auditores. Veremos las pruebas y revisiones que se deben realizar en la auditoría de la seguridad física, de una manera más concreta y práctica en el siguiente capítulo de este trabajo.

Podemos hacer, no obstante, una pequeña clasificación de las áreas más comunes que se suelen diferenciar, estas son **las instalaciones**, **la producción** y **el desarrollo**.

Algo muy importante y que nos va a proporcionar mucha información es **la observación.** Ésta se deberá llevar a cabo durante todo el proceso de auditoría, sobre todo al comienzo de ésta, ya que si no nos identifican como auditores veremos las

situaciones cotidianas que se viven en la entidad, debido a que cuando los empleados saben que se está realizando la auditoría, cumplen mejor las normas. La observación no figura en los manuales ni en los planes de trabajo, pero el auditor con experiencia debe estar atento para recabar la máxima información posible en todo momento.

Por ejemplo, mientras se está revisando la configuración de un determinado sistema, el auditor podrá comprobar si se cumplen otras normas, como si tiene las contraseñas escritas en *post-it´s*, si existen indicios de que se fuma en el centro computacional, si hay migas o restos de comida, si acceden al centro personas que no deberían, etc.

i) Las instalaciones

Las instalaciones en sí, como hemos comentado en el capítulo anterior (Seguridad Física) están muy relacionadas con los sistemas informáticos de la entidad. Es por este motivo que se deberán hacer las pruebas y revisiones correspondientes en cada caso. Veremos mucho más en profundidad en el siguiente capítulo las revisiones que se tienen que realizar en las instalaciones para analizar la seguridad física de los sistemas informáticos.

ii) La producción

Dado que se sale del contexto de este trabajo, vamos a ver rápidamente las pruebas que se suelen realizar en el ámbito de la producción. En el siguiente capítulo veremos las revisiones que se deben realizar a éstos sistemas en lo que a Seguridad Física se refiere.

ii.i) Configuraciones y arquitecturas empleadas.

ii.ii) Análisis de software. Aplicaciones, paquetes, etc.

ii.iii) Análisis de redes y comunicaciones en general.

ii.iv) Clasificación de la información.

ii.v) Planes de seguridad, de contingencia, etc.

ii.vi) Registros de visitas.

ii.vii) Matriz de accesos y paquetes de seguridad.

ii.viii) Gestión de problemas y cambios.

iii) El desarrollo

Al igual que ocurre con la producción, vamos simplemente a mencionar los aspectos más importantes que se deben revisar y veremos en el siguiente capítulo las medidas de Seguridad Física que, en su caso, deben tener.

iii.i) Cartera de pedidos y prioridades.

iii.ii) Metodologías, ciclos, normas, etc.

iii.iii) Documentación en general.

d) Fuentes externas a la entidad

Entendemos por fuentes externas a la entidad como aquellas entidades o personas que han tenido relación con ésta y nos pueden aportar información, como clientes, proveedores, colaboradores, entidades subcontratadas, etc. Puesto que, en principio, no les afecta la auditoría, la información que nos proporcionen será objetiva e independiente, por lo que se deberán tener en cuenta en el desarrollo de la auditoría.

3.4.3 - El informe

El informe es el resultado de la auditoría. Es la valoración por escrito de la situación observada, recogiendo las debilidades, los riesgos y las posibles mejoras. Es la comunicación formal y oficial con los auditados y con la dirección. Como vamos a ver a continuación, el desarrollo del informe tiene varias fases, **análisis de la información**, realización de un **borrador del informe** y realización del **informe definitivo**.

a) Análisis de la información

Una vez que se ha recopilado la información suficiente durante el trabajo de campo, se debe proceder al análisis de la misma, ésta se puede clasificar en dos grupos, la **documentación permanente** y los **papeles de trabajo**. Con el análisis de la información lo que se pretende clasificarla y organizarla para obtener una idea clara de las debilidades, riesgos y vulnerabilidades de la entidad auditada y así poder llegar a unas conclusiones concretas que proporcionen las recomendaciones adecuadas.

El primer aspecto que se debe observar es si se dispone de las **evidencias suficientes** para poder llegar a una conclusión concreta. Esto es muy importante, ya que el informe que realicemos debe estar apoyado fuertemente por la información que hemos ido recabando. Si no disponemos de estas evidencias, deberemos realizar de nuevo un pequeño trabajo de campo más concreto, que nos permita obtenerlas.

i) Archivo permanente

Entendemos por archivo permanente toda la documentación que hemos obtenido de la entidad, como puedan ser organigramas, planes de sistemas informáticos, pólizas de seguros, etc. Aunque se dice que es permanente, es necesario que se actualice cuando se produzcan variaciones (contratos, organigramas, configuraciones, etc.), así como verificar que están vigentes y son completos.

ii) Papeles de trabajo

Los papeles de trabajo son la documentación del proceso de auditoría, de los procedimientos seguidos, los cuestionarios y entrevistas, las pruebas realizadas, la información recogida y las conclusiones a las que se han ido llegando. Podemos decir, por tanto que los papeles de trabajo son los documentos que han manejado y creado los auditores, como pueden ser cartas y memorandos, listas de comprobación, cuestionarios, notas tomadas, listados y actas, comentarios de los auditores y conclusiones, así como cualquier otro documento relacionado.

Puesto que pueden ser la **única defensa del auditor**, aparte de ser útiles para justificar su trabajo, para revisar conclusiones, e incluso, para la formación de auditores *junior*, los papeles de trabajo deben cumplir unos requisitos y **características** concretas. Vamos a verlos a continuación. Además deberá estipularse en cada caso el tiempo que se han de guardar. Si bien es recomendable que se almacenen durante un periodo de varios años, en algunos casos las entidades auditadas prefieren que se destruya toda la información relacionada con el proyecto.

ii.i) Completos
Los papeles de trabajo deben estar completos, no se debe eliminar ningún dato obtenido. Deben incluir toda la información obtenida, las fuentes, las conclusiones, etc. Además no se deben dejar cabos sueltos ni posibles vacíos que puedan originar dudas.

ii.ii) Exactos
Es muy conveniente que el auditor aclare por escrito cómo ha verificado las pruebas contenidas en los papeles o que puedan derivarse de éstos.

ii.iii) Claros y fáciles de entender
Deben ser fáciles de entender también por otras personas, por lo que siempre que sea posible deben usarse formularios estándar o que al menos respondan a formatos predeterminados. Deben evitarse los papeles manuscritos, que pueden conservarse como anexo, pero cuya trascripción a ordenador debe hacerse lo antes posible.

ii.iv) Numerados y clasificados
Cada papel de trabajo deberá tener un identificador único y deben existir varios índices para facilitar su manejo. Algunos de estos índices podrían ser por áreas, por autor, cronológicos, por importancia, etc.

b) El desarrollo del informe

Tras todo el proceso de auditoría, el informe es el único producto perdurable y por el que juzgarán a los auditores y tal vez, pasado el tiempo. La obsesión lógica de los auditados durante todo el proceso de auditoría habrá sido tener un informe positivo o, al menos, benigno, ya que esto puede traducirse en evitación de conflictos y, tal vez, en reconocimiento y recompensa. Por otro lado, la obsesión del auditor será la de producir un informe objetivo, veraz y útil que suponga una aportación para la entidad. En ocasiones, estas dos obsesiones resultan contrapuestas.

Como ya hemos comentado, existen dos informes distintos, o mejor dicho, dos versiones del informe, el borrador y el definitivo. Vamos a ver a continuación aspectos y generalidades comunes a ambos y más adelante las particularidades que tiene cada uno.

i) Características del informe

Como ya hemos dicho, vamos a ver las características y estructura del informe, que datos debe aportar y cómo hacerlo.

i.i) Contenido y enfoque
Lógicamente, el contenido del informe y el enfoque que se le dé, dependerá básicamente del objetivo y ámbito de la auditoría.

i.ii) No hablar de personas
Es importante que en el informe no nos refiramos a personas en concreto, en todo caso, nos referiremos a puestos o funciones.

i.iii) Incluir puntos positivos
El hecho de incluir algunos puntos positivos, que siempre suele haberlos, denota que el informe no es exclusivamente una relación de "puntos negros", y anima a las auditaos. En todo caso, y pensando sobre todo en que pueden leerlo directivos no familiarizados con la auditoría informática, no está de más incluir algún párrafo aclarando que el informe se refiere a los puntos susceptibles de mejora o de un mayor control, obviando los que están dentro de la normalidad.

i.iv) Explicaciones no técnicas
Es probable que el informe lo lea la alta dirección o el comité de auditoría y que no estén familiarizados con términos técnicos, pero es necesario que entiendan la esencia de lo expuesto en el informe. Por tanto se debe realizar alguna acción para pueda ser comprendido. Las más usuales son la de incorporar una carta adjunta con las explicaciones oportunas dependiendo de a quién vaya dirigido, realizar un capítulo de resumen de diagnóstico sin términos técnicos o realizar dos volúmenes del informe, uno detallado con datos técnicos y otro resumido.

i.v) Incluir recomendaciones, no reglas
En el informe se debe hablar en todo momento de recomendaciones pero nunca de reglas u obligaciones.

i.vi) Rigor, calidad, claridad y precisión
El informe debe tener rigor, claridad, calidad y precisión en sus datos, conclusiones, comentarios y recomendaciones.

ii) Estructura del informe

La estructura del informe se divide en tres partes, la **introducción**, el **cuerpo** y los **anexos**. Vamos a ver la estructura de cada una de éstas, así como los puntos principales con los que deben contar.

ii.i) Introducción

La introducción del informe destacará los aspectos más importantes de éste y pondrá al corriente de las peculiaridades concretas de la auditoría. Debe contener los siguientes puntos.

ii.i.i) Índice
El índice no es necesario si el informe tiene pocas páginas.

ii.i.ii) Conclusiones y resumen
Se deben incluir al principio del informe las conclusiones principales a las que se han llegado con la realización de la auditoría, así como un pequeño resumen de la misma. Con esto conseguiremos poner en situación al lector del informe y que éste sea más fácil de comprender.

ii.i.iii) Antecedentes
Siempre que existan antecedentes se deben comentar, de esta manera podremos justificar ciertas pruebas, verificaciones o recomendaciones.

ii.i.iv) Objetivo y ámbito de la auditoría
Se debe indicar cual es el objetivo de la auditoría y cual ha sido el ámbito en el que se ha desarrollado. De esta manera centraremos la atención de las recomendaciones y justificaremos el enfoque dado en el informe. En ocasiones el objetivo principal de la auditoría no se manifiesta a los auditores y queda en las mentes de quienes la encargan o, como hemos comentado anteriormente, se dice pero no deba especificarse como tal en los informes, sobre todo si la auditoría tiene como objetivo evaluar a personas en concreto.

ii.i.v) Agradecimientos
En el caso de proceda, se deben incluir los agradecimientos oportunos.

ii.i.vi) Descripción del entorno informático
La descripción de las instalaciones puede comenzar con alguna referencia a la entidad, a su posicionamiento en el mercado, al sector, al grupo de entidades, etc. Ya que ello puede influir o tener relación con la situación de la informática y su evaluación, así como riesgos específicos del sector, crisis relacionadas con la tecnología obsoleta, etc. Respecto a las instalaciones propiamente dichas, debe hacerse una pequeña descripción para confirmar que las bases de partida han sido correctas, tales como equipos, comunicaciones, software, etc.

ii.i.vii) Limitaciones de la auditoría
En el caso de existir, se deben incluir las limitaciones de la auditoría. Éstas pueden ser totales, si la auditoría no se ha podido finalizar, o parciales, que es lo más habitual. Las limitaciones parciales pueden tener su origen en documentación que se ha solicitado pero a la que no se ha tenido acceso, personas a las que no se ha podido entrevistar, instalaciones que no se han visitado, dificultades propias del entorno, como lenguajes específicos o documentación en otro idioma, etc.

ii.ii) Cuerpo del informe

En el cuerpo del informe es donde vamos a incluir todos los puntos que creamos oportunos de mención en la auditoría informática. Generalmente, cada punto que tratemos se corresponderá con una deficiencia encontrada y se deberán incluir tantos creamos conveniente, así como un pequeño resumen al que llamaremos cuadro final. Vamos a ver a continuación como se deben estructurar los puntos que mencionemos y que debe incluir cada uno de ellos, así como el cuadro final.

ii.ii.i) Estructura del cuerpo del informe

Algunos auditores estructuran el cuerpo del informe por tipos de control (controles administrativos, de seguridad, etc.) pero en la práctica suele ser preferible estructurarlo por áreas (desarrollo, explotación, etc.) y con posibles desgloses por grupos en el caso de instalaciones complejas, de ese modo se facilitará la discusión con auditados y la distribución y seguimiento de los puntos a los responsables de la entidad.

Otro aspecto que se debe tener en cuenta es la agrupación de los puntos que sean homogéneos. Aunque cada punto en concreto debe contar con los puntos que vamos a ver a continuación, es posible que varios estén estrechamente relacionados, llegando incluso a tener el mismo origen o recomendación. De ser así, se deberán agrupar los puntos homogéneos para facilitar la comprensión del informe, así como la implantación de las recomendaciones.

ii.ii.ii) Qué incluir en cada punto

En cada punto o grupo de puntos, en el caso de haber agrupado varios de éstos suficientemente homogéneos, se deberán incluir los siguientes aspectos.

ii.ii.ii.i) Descripción de la deficiencia

Se debe realizar una descripción precisa de la deficiencia observada.

ii.ii.ii.ii) Causa de la deficiencia

Debemos anotar cuál es la causa de la deficiencia que estamos tratando, y si lo creemos oportuno podemos hacer referencia a la documentación en la que nos basamos.

ii.ii.ii.iii) Efecto

Se debe anotar el efecto que puede tener esa deficiencia para los sistemas informáticos de la entidad, así como su importancia y riesgo.

ii.ii.ii.iv) Recomendación

En cada punto o grupo de puntos debe incluirse una recomendación que sea viable para el tipo de instalación. Muy excepcionalmente la recomendación puede consistir en que la entidad o expertos externos realicen un estudio sobre las soluciones más adecuadas, si los auditores están limitados por la complejidad del entorno o sus características para haces una recomendación específica.

ii.ii.iii) El cuadro final

Tras haber expuesto todos los puntos en el cuerpo del informe y a modo de resumen de los puntos tratados, podemos incluir un cuadro final, sobre todo si son muchos puntos o si se desea destacar la importancia de unos frente a otros. En cualquier caso, suele ser útil incluir un cuadro final donde se recojan las recomendaciones, y con la sugerencia de prioridad, ya que la prioridad definitiva la tomará la dirección de la entidad auditada.

Normalmente el cuadro final recoge los siguientes aspectos de cada punto.

ii.ii.iii.i) Prioridad de los puntos
Como acabamos de comentar, debe incluir una recomendación de prioridad entre las debilidades que se deben abordar.

ii.ii.iii.ii) Clasificación por áreas
Se puede hacer una clasificación por áreas de los distintos puntos a tratar.

ii.ii.iii.iii) Destacar los más importantes
Al margen de la recomendación de prioridad, se puede destacar de algún modo los puntos que consideremos que son más importantes.

ii.ii.iii.iv) Nivel de riesgo
Puede que aunque no sean los más importantes, entrañen un riesgo alto o concreto, por lo que se deberá indicar el nivel de riesgo que entraña para la entidad cada punto.

ii.ii.iii.v) Esfuerzo y coste
Es conveniente incluir el esfuerzo y coste que va a suponer para la entidad auditada la implantación de la recomendación dada para cada punto en concreto. El riesgo, el esfuerzo y el posible coste pueden orientar la asignación de prioridades, y abordar en primer lugar lo que tenga un mayor riesgo y a la vez un coste y esfuerzo menores.

ii.iii) Anexos

En ocasiones, y dependiendo del ámbito y profundidad de cada auditoría en concreto, puede que no se incluyan anexos en el informe. No obstante, es preferible mover a este apartado todo aquello que pueda desviar la atención de quien lee el informe, aunque se hagan en éste referencias al contenido del anexo, como por ejemplo, las listas de parámetros expandidas, planos, etc. Además se debe incluir en los anexos toda la información que pueda interferir o engordar demasiado el cuerpo del informe.

En el anexo, por tanto, incluiremos los documentos necesarios para demostrar afirmaciones o aportar información a lo tratado en el cuerpo del informe. Vamos a ver cuales son los documentos que generalmente se deben incluir en el anexo.

ii.iii.i) Entrevistas y contactos
Algo conveniente es incluir en el anexo la lista de personas a las que se ha entrevistado, si bien se debe hablar de funciones o puestos y no de personas, ya que se podrían sentir molestas. Si solo existiera una única persona por función o puesto, el problema seguirá persistiendo, pero lo que es imprescindible es que los auditores guarden en sus papeles los listados de quién dijo qué y cuándo lo dijo.

ii.iii.ii) Cuestionarios y resultados
Cuando aporten información extra, apoyen las recomendaciones o sean la causa de las deficiencias, es conveniente incluir cuestionarios y resultados de pruebas realizadas.

ii.iii.iii) Documentación empleada
Al igual que con los cuestionarios y resultados, es conveniente incluir la documentación que consideremos más relevante.

ii.iii.iv) Gráficos
Cuando en el informe se incluyan gráficos o visuales, deberán estar en el anexo, con la referencia desde el punto o apartado correspondiente.

ii.iii.v) Listados
Se deberá valorar si se incluyen listados. De incluirse, éstos no deben ser muy voluminosos y sólo si son imprescindibles para demostrar algo importante y concreto.

iii) Otros aspectos del informe

Existen ciertas medidas de seguridad e integridad que es conveniente adoptar, sobre todo si el informe tiene una gran trascendencia, incluso relacionado con delitos o fraudes o bajo rendimiento y que pueden derivar en despidos e incluso en acciones legales. Vamos a ver las principales medidas que se pueden adoptar en estos casos.

iii.i) Proteger contra escritura
Una opción para evitar que se elimine, sustituya o modifique alguna hoja o párrafo del informe es protegiéndolo contra escritura. Ésta es una medida que se debe emplear en los casos de gran trascendencia que hemos comentado.

iii.ii) Incluir en sus hojas información
Se puede incluir en cada una de las hojas información acerca del documento que dificulte el uso indebido de éste. Lo más usual es incluir en cada página, como título o a pie de página, la entidad, el número de trabajo y la fecha, entre otros datos que se crean oportunos.

iii.iii) Leyenda de confidencial
Se debe incluir, en la portada o en cada una de las páginas la leyenda CONFIDENCIAL.

iii.iv) Leyenda de borrador
Cuando el informe sea el borrador, se deberá incluir en la portada o en cada una de sus páginas la leyenda BORRADOR.

iii.v) Firma de auditores
Es conveniente que los auditores firmen en, al menos, una de las páginas del informe.

iii.vi) Número de página
Se debe incluir en cada página del informe el número de página y el número de páginas totales, de esta manera nos percataremos rápidamente si se sustraen páginas del informe.

iii.vii) Número de copia y destinatario
Otra medida de seguridad que se puede incluir es la de anotar en cada página el número de copia del informe y, en su caso, quien es el destinatario, así, si se realizan copias del informe podremos saber cual ha sido el original desde el que se ha filtrado.

iv) El borrador

Como hemos comentado, para realizar el informe definitivo **es imprescindible que se elabore antes un borrador** del mismo, para que los auditados lo examinen y puedan rebatir ciertas cuestiones que consideren que no son acertadas. El borrador debe ser, en principio, igual que el definitivo, contar con la misma estructura, los mismos puntos, etc. Vamos a ver los procesos de creación y los aspectos más importantes del borrador.

iv.i) Revisión
Debe realizarse una revisión del borrador del informe, además de por parte del gerente o jefe de auditoría, por personas ajenas al proceso, como otro jefe o gerente.

iv.ii) Entrega a los auditados
Se bebe entregar una copia a los auditados, normalmente al departamento que ha encargado la auditoría o al director de informática, para que lo revise y analice.

iv.iii) Sesión de discusión
Una vez que los auditados han tenido tiempo de analizar y revisar el borrador del informe (en ocasiones el borrador se les entrega en la misma sesión de discusión), se debe realizar una sesión de discusión con el fin de contrastar el contenido y aclarar malentendidos. En esa sesión, que pueden ser varias, deben aclararse totalmente los puntos, aportando evidencias tanto auditados como auditores, éstos aportando la documentación recabada y los papeles de trabajo, hasta llegar a acuerdos. Esto no debe suponer que los auditores cedan en sus opiniones si no se les demuestra fehacientemente que estaban equivocados. Es más normal que se admita algún cambio de palabras o frases a sugerencia de los auditados, si con ello no se ve afectada la esencia de los puntos indicados.

v) El informe definitivo

Una vez que se han esclarecido todos los puntos en la sesión de discusión, se elaborará el informe definitivo, en éste se pueden incluir las modificaciones que se han hecho respecto al borrador y porqué. Vamos a ver los aspectos más relevantes del informe definitivo.

v.i) Entrega del informe
Un aspecto importante es la entrega del informe al cliente, se debe valorar si se hará personalmente o por correo, y si es así, las medidas de seguridad que se tomarán al respecto. En el caso de los auditores externos, el informe se debe entregar a quien haya encargado el trabajo, y si existe un departamento de auditoría se le debe entregar una copia. De no existir, y si esa es la norma de la entidad, se le puede entregar al comité de

informática, sistemas de información o dirección. En el caso de los internos, se le entregará a quien esté establecido según las normas de la entidad.

v.ii) Presentación
Si es requerido o se ha establecido de antemano, se podrá realizar una presentación del informe a los auditados, para explicar así, los puntos, la prioridad, etc., facilitando de esta manera la comprensión del informe.

v.iii) Implantación de las soluciones
En cualquier caso, la entidad auditada, y a un nivel suficientemente alto, decidirá que hacer con respecto a las debilidades y aspectos a mejorar señalados y la prioridad de éstos, normalmente en base a la importancia y urgencia indicada por los auditores en su informe, además de con qué medios se realizarán. A veces es aconsejable el apoyo externo para no interrumpir proyectos en curso ni retrasar la implantación de las soluciones a los problemas detectados.

v.iv) Seguimiento
Por parte de los internos, y excepcionalmente y si se ha estipulado, por parte de los externos, deberá haber un seguimiento de la implantación de las recomendaciones, elaborando informes periódicos.

4 - AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA

4.1 - Introducción

Como hemos comentado en el capítulo anterior, la auditoría informática se puede realizar de cualquier aspecto, programa, sistema o dispositivo en concreto que tenga alguna relación directa o indirecta con la informática o los sistemas de información. En este caso vamos a ver los riesgos y vulnerabilidades que pueden afectar a la **Seguridad Física** en concreto, a sí como las medidas o pautas que se deben seguir para proteger nuestros sistemas.

Por tanto, la Auditoría Informática de la Seguridad Física va a ser un proceso de auditoría informática, como el descrito en el capítulo anterior, pero centrando sus análisis y revisiones en los aspecto mencionados en el capítulo 2 - Seguridad Física.

El objetivo de este trabajo es el de poder dar una evaluación del nivel de Seguridad Física que tienen los sistemas de información, por tanto, analizaremos los riesgos y amenazas principales, ya que el ámbito es muy grande y queda muy abierto a las condiciones concretas de la entidad a auditar.

Por ejemplo, si un empleado de una gran entidad, que en principio puede parecer *poco importante*, maneja información relevante o importante, como puede ser la gestión de nóminas, y la almacena en su PC, realizando o no copias en el servidor de datos, estaríamos hablando de un problema de gestión o formación, pero en cualquier caso perteneciente al ámbito de la **seguridad lógica**. Por tanto, aunque en ese PC se almacene información importante o delicada, se sale del alcance de este trabajo el verificar que dicho PC cumple todos los requisitos de Seguridad Física de los que vamos a hablar para, por ejemplo, los servidores de datos ubicados en el centro computacional.

Lo que vamos a tratar en este trabajo, por tanto, es la revisión de la Seguridad Física de los sistemas más importantes, relevantes o delicados en una entidad como pueden ser los servidores de datos, las copias de seguridad, los dispositivos de red, los canales de comunicaciones, etc.

Obviamente, dependerá de la entidad en concreto y de las necesidades y criticidad de los datos o sistemas. En este trabajo se va a hacer una revisión general de los sistemas más comunes para una entidad de un tamaño medio o grande. En cada caso concreto se tendrán que adaptar las revisiones, los cuestionarios y, en general, la forma de actuación.

Hemos hablado ya del **centro computacional** o centro de cómputo, que es donde en una entidad se disponen los elementos informáticos más críticos para ésta, como las consolas de administración, los dispositivos de red, los servidores de datos y aplicaciones, etc. por tanto nuestros esfuerzos se centraran en revisar la Seguridad Física de este lugar, haciendo una revisión general y más relajada del resto de equipos o sistemas, llamados de usuario final, y que siguiendo una buena política de seguridad lógica, su pérdida no deberá suponer para la entidad más que su valor económico.

Lo primero que vamos a hacer es el desarrollo de un **cuestionario**, que será la base de nuestra investigación ya que nos va a indicar todos los aspectos que se deben revisar en la auditoría. Como veremos más adelante, podrán contestar a las preguntas los propios empleados, tanto por escrito como por medio de entrevistas, pero deben ser los auditores los que por medio de pruebas y verificaciones contesten a las preguntas del cuestionario en última instancia, de esta manera se obtendrán unas respuestas más objetivas e independientes.

4.2 - Trabajo preparatorio

Como en toda auditoría informática, debe existir un trabajo previo, que debe de constar de los puntos que hemos comentado en el capítulo anterior. Para el caso de la Auditoría Informática de la Seguridad Física no se dan unos requisitos o características concretas de este trabajo, por lo este proceso seguirá ya expuesto sobre el trabajo preparatorio, y contará, por tanto, con las siguientes fases.

a) Encargo del trabajo

b) Planificación

c) Programa de trabajo

4.3 - Recopilación de información

Vamos a ver, de las distintas fuentes de las que podemos obtener información, como son la **documentación**, el **personal**, las **revisiones y pruebas** y las **fuentes externas a la entidad**, las que más nos pueden interesar en cada caso, así como cómo podemos obtener la información concreta para nuestra revisión de la Seguridad Física.

Como ya hemos comentado en el capítulo anterior, es conveniente disponer de un **cuestionario** para evitar que se nos pueda pasar algún punto por alto. Normalmente se dispondrá de un cuestionario general que se deberá adaptar dependiendo del objetivo, ámbito y profundidad de la auditoría, así como de la entidad auditada en concreto. En este trabajo se ha desarrollado un cuestionario donde se tratan todos los aspectos de la Seguridad Física que hemos ido viendo (capítulo 5 - El cuestionario).

De esta manera, el cuestionario nos va a ser útil para recopilar información **del personal**; podremos entregar el cuestionario a los empleados para que lo rellenen, así como realizar nosotros mismos las preguntas en una entrevista anotando las respuestas obtenidas. También lo utilizaremos nosotros mismos obteniendo las respuestas mediante **pruebas y comprobaciones**.

4.3.1 - La observación

Como ya hemos comentado, la observación es muy importante y debe desarrollarse a lo largo de todo el proceso de auditoría. Lo situamos en primer lugar porque existen ciertas revisiones o verificaciones que exigen un alto grado de **factor sorpresa**, ya que es

normal que cuando los empleados saben que se está realizando la auditoría, traten de seguir mejor las normas.

Por ello, intentaremos recabar la máxima información realizando observaciones, que no constarán en los planes de trabajo, pero que quedarán a juicio del auditor. De esta manera, simplemente deambulando por las instalaciones de la entidad, podremos recabar la máxima información posible. Hay que hacer hincapié en que en esta fase únicamente se revisarán los aspectos que requieren un alto grado de factor sorpresa, dejando para más adelante el resto, que se llevarán a cabo siguiendo la planificación establecida. Vamos a ver los principales aspectos a revisar en esta fase.

a) Acceso al edificio

Se deberá intentar acceder a las instalaciones sin identificarnos como auditores, tanto por la entrada principal como por otras que pudiéramos encontrar. Se deberán anotar todos los controles por los que pasamos, y si finalmente conseguimos acceder. Es posible que en entidades grandes exista la posibilidad de que en la entrada principal nos den el alto y podamos acceder como visitantes. No debemos revelar nuestra identidad para así proseguir con nuestra investigación.

b) Interior del edificio

Si hemos conseguido acceder al edificio, tanto si lo hemos hecho como intrusos como si lo hemos hecho como visitantes, deberemos realizar algunas comprobaciones más en el interior de éste. Si por el contrario no hemos podido tener acceso a las instalaciones, los puntos que detallamos a continuación los deberemos comprobar, en la medida de lo posible, durante el proceso de auditoría.

i) Dispositivos eléctricos
Un aspecto en el que nos podemos fijar es en los sistemas eléctricos. No es muy extraño que dispositivos tales como los enchufes o cuadros de fusibles se encuentren totalmente accesibles. Deberemos tomar nota sobre su estado, ya que es normal que los enchufes se encuentren deteriorados por encontrarse en el suelo. Además nos fijaremos en si está muy extendido el uso de ladrones o alargadores por parte de los usuarios, así como si están bien instalados, si los cables están canalizados, etc.

ii) Dispositivos de red
Se deberá comprobar si los cables de red están bien instalados o si por el contrario, por haberse realizado modificaciones en la ubicación de los sistemas existen largos cables por el suelo o paredes sin ninguna canalización que los proteja. Se podrá verificar además el estado de las tomas de red o rosetas, la accesibilidad a éstas, etc.

iii) Limpieza
Se deberá inspeccionar el grado de limpieza general de las instalaciones, sobre todo en el entorno del hardware. Se comprobará si existe mucho polvo, suciedad, etc.

iv) Sistemas antiincendio

Aunque se revisarán de manera más exhaustiva en el momento correspondiente, se debe hacer una pequeña revisión visual de los sistemas antiincendio, generalmente de los sellos y fechas de revisión de los extintores portátiles y de la accesibilidad y visibilidad de los mismos, ya que no es extraño que se encuentren tapados por cajas o materiales, e incluso, detrás de armarios.

v) Acceso a zonas protegidas y cerradas
Intentaremos acceder a zonas protegidas, como el centro de cómputo, o cerradas, como pudiera ser un almacén donde se guardan equipos informáticos y que debería estar cerrado. En general, intentaremos llegar lo más lejos posible. Se anotarán los controles que hayamos podido sufrir, así como hasta donde hemos podido llegar.

c) El entorno del hardware

Es posible, y deseable, que el acceso al entorno más directo del hardware no nos haya sido permitido, no obstante se deben levar a cabo ciertas observaciones que, de no poder realizarse en este momento se deben realizar a lo largo del proceso de auditoría. De cualquier manera, vamos a ver los puntos más importantes que debemos revisar.

i) Puertas abiertas
Se revisará si los empleados que tienen acceso al centro computacional dejan, normalmente, las puertas abiertas, así como si empleados que no tienen acceso a éste acceden con regularidad.

ii) Temperatura
Aunque se revisará más exhaustivamente cuando corresponda, se debe hacer comprobar que los sistemas que precisan una ventilación adecuada se encuentran aislados del resto, normalmente mediante mamparas. No es extraño que éstas se encuentren abiertas para comodidad de los empleados que deben manejar estos sistemas.

iii) Comida y bebida
Es posible que la entidad permita comer o beber en el centro de cómputo, de ser así una posible recomendación final sería que se prohibiera. En cualquier caso, se deberá revisar si existen indicios, más o menos claros de que se coma o se beba en el centro computacional.

iv) Tabaco
Como ya se ha comentado en el capítulo de Seguridad Física, con entrada en vigor de la **LEY 28/2005, de 26 de diciembre, de medidas sanitarias frente al tabaquismo** el 1 de enero de 2006, queda prohibido fumar en los centros de trabajo en general, y por tanto en el centro computacional. Aún así, se debería verificar el cumplimiento de dicha ley, especialmente en el entorno más directo del hardware. Para realizar esta observación es necesario un alto grado de factor sorpresa, aunque se pueden indagar indicios, como ceniceros, colillas o ceniza.

v) Limpieza

Como ya hemos comentado, la limpieza es un aspecto importante, especialmente en el entorno del hardware. Por tanto, se deberá revisar y tomar nota del nivel de limpieza que existe.

4.3.2 - La documentación

La documentación que se debe solicitar a la entidad auditada dependerá en función de los objetivos, ámbito y profundidad de la auditoria en concreto, pero a rasgos generales, se deben solicitar los siguientes documentos para más adelante proceder a su análisis y revisión. Más adelante los principales aspectos que se deben analizar de cada documento solicitado.

i) Organigrama de la entidad y funciones
Analizar cual es la dependencia de la entidad de la informática, verificar que existe un departamento de seguridad informática. Si existe un departamento de auditoría, verificar que no depende en ningún caso del departamento de informática ni de ninguno de sus directores y que los integrantes de este departamento no participan en el desarrollo, mantenimiento, seguridad o ninguna otra tarea que puedan auditar.

ii) Políticas y procedimientos
Se debe verificar que existen políticas de gestión y actuación y que los procedimientos que emplea la entidad en lo que a sistemas informáticos son los adecuados. De no existir políticas o procedimientos se debe recomendar su creación, y en cualquier caso, que sean los idóneos para la entidad en concreto y que se han tenido en cuenta los estándares aplicables (ISO´s, UNES, etc.).

iii) Planes de seguridad
Verificar que existe un plan de seguridad adecuado para la entidad en concreto, real y factible. Se debe, además, verificar que la realidad se ajusta en lo establecido en el plan de seguridad y que el personal que, de algún modo, esté relacionado con el plan de seguridad está al tanto de éste y debidamente formado para llevarlo a cabo. De no existir se debe recomendar su creación.

iv) Planes de contingencia
Verificar que existe un plan de contingencia adecuado para la entidad y que la realidad de la entidad se ajusta con lo establecido en el plan de contingencia, de no ser así se deberá modificar para que se adecue a las necesidades de la entidad y para que se cumpla lo estipulado en éste. De no existir se debe recomendar la creación de uno.

v) Actas de comités
Analizar las decisiones tomadas con respecto a los sistemas informáticos de la entidad, para poder hacernos una idea del posible origen de las debilidades que encontremos.

vi) Memoranda y comunicados
Es importante conocer los memorandos y comunicados que la entidad envía a sus empleados con respecto a las medidas de seguridad en general, y a las de seguridad física en concreto, que deben adoptar con respecto a las sistemas informáticos y de información, ya que es muy importante que los empleados en general tengan una formación y conocimientos mínimos sobre éstos sistemas. De no ser así podrían poner

en grabe peligro, muchas veces por desconocimiento, la seguridad de los sistemas informáticos y de la información en general. Además, analizando estos documentos podríamos encontrar el origen de ciertas debilidades encontradas en la entidad.

vii) Planos de las instalaciones
En muchos aspectos de la Seguridad Física se tienen que tener presentes los planos de las instalaciones. Se deben solicitar y tenerlos presentes durante todo el proceso de auditoría, para de esta manera poder consultarlos cuando sea necesario. En principio, todas las entidades contarán con los planos de sus instalaciones, de no ser así se deberá pedir una copia en el organismo correspondiente.

viii) Contratos
Se deberán pedir los contratos del personal que tenga una relación directa con los sistemas informáticos o con la información más relevante para la entidad, para poder revisar las cláusulas que existen con respecto a la confidencialidad y tratamiento de datos. De no existir dichas cláusulas se debe recomendar que se creen y se implanten.

ix) Pólizas de seguros
Se deben solicitar todas las pólizas de seguros y revisar qué sistemas o dispositivos están protegidos, si se tienen asegurados los datos por un cierto valor económico y las situaciones o riesgos que cubren los seguros, como incendios o inundaciones, y si dependiendo del origen de los mismos puede la aseguradora no hacerse responsable del pago. Se revisará que todos los dispositivos, sistemas e incluso, los datos, estén debidamente cubiertos. Si se ha observado que la entidad tiene un probabilidad alta ante un riesgo en concreto, como que se encuentre ubicada en una zona propensa a sufrir inundaciones, se debe hacer hincapié en que este factor esté completamente cubierto en las pólizas de seguros.

x) Informes anteriores
Si existen, los informes de auditorías anteriores, de cualquier aspecto de los sistemas informáticos y especialmente de la Seguridad Física, nos permitirán conocer las debilidades que se encontraron en la entidad, y por tanto, verificar si se han solucionado, o si por el contrario el problema persiste aún. Nos permitirán además estar al tanto de lo acontecido en la entidad y nos aportará información adicional que hayamos podido pasar por alto.

4.3.3 - Análisis del entorno de las instalaciones

Como hemos comentado en el capítulo de Seguridad Física, el entorno de las instalaciones nos va a determinar el nivel de riesgo que suponen las distintas amenazas. Por tanto, se deberá realizar un estudio del entorno de las instalaciones para conocer ante qué amenazas debemos hacer un mayor esfuerzo en seguridad y cuales nos van a afectar poco o muy poco, y por lo tanto podremos instalar sistemas de seguridad más relajados. No obstante, al margen de este pequeño estudio, se podrá recabar más información al respecto incluyendo preguntas relacionadas en cuestionarios y entrevistas.

Se deben analizar, por tanto, todos los factores, tanto naturales como no naturales y sociales que vamos a comentar a continuación. Una buena técnica es **cuantificar el**

riesgo que supone para le entidad una cierta amenaza, así podremos conocer en qué medidas de seguridad se debe hacer un mayor esfuerzo y cuales pueden ser más suaves. Para ello, mediante el estudio de cada amenaza en concreto, y aunque para cada entidad puede variar el estudio, vamos a ver los aspectos generales que se deben analizar. Tras el estudio se debe llegar a una conclusión respecto al nivel de riesgo que supone, que en nuestro caso podrá adoptar los valores de muy bajo, bajo, normal, alto y muy alto.

a) Naturales

i) Terremotos
En general, en cualquier punto de la península van a suponer un riesgo muy bajo, no obstante se debe investigar si la zona geográfica en la que se encuentra la entidad tiene cierta actividad sísmica, para ello debemos indagar en posibles antecedentes de terremotos en la zona.

ii) Tormentas eléctricas
Existen ciertas estadísticas, tanto oficiales como extraoficiales, que indican el número de rayos que han caído en una determinada zona. Al margen de esto, prácticamente toda la superficie de la península ibérica está expuesta a sufrir una tormenta eléctrica, sobre todo en épocas calurosas y secas.

iii) Temperatura
Como ya hemos comentado, las altas temperaturas afectan muy negativamente a los sistemas electrónicos en general, y a los informáticos en particular, por lo que se deberá realizar un pequeño estudio acerca de las temperaturas que se dan a lo largo del año en la zona, tanto máximas como medias. En verano, en casi cualquier punto de la península ibérica se alcanzan altas temperaturas.

iv) Humedad
Dado que la humedad varía mucho dependiendo de múltiples factores, como la época del año, o la vegetación de la zona, por tanto se deberá recurrir a estadísticas acerca del nivel de humedad que se da en la zona en concreto.

v) Lluvias
Éstas varían también dependiendo de la época del año, por lo que de nuevo se deberá recurrir a muestreos y estadísticas que nos permitan conocer cuales son los niveles que se dan en la zona. Además, deberemos investigar la ubicación de la entidad: si se encuentra en una depresión del terreno, en una antigua zona de paso de agua, la cercanía con ríos y arroyos, etc.

b) No naturales

i) Vibraciones
En general, se podrá observar si existen elementos externos que puedan originar vibraciones en el interior de la entidad, tales como carreteras o maquinaria pesada que opere cerca de las instalaciones. Si por el objetivo de la auditoría es preciso, o si se considera oportuno, se pueden realizar estudios más exhaustivos mediante sistemas que analicen el nivel de vibraciones que sufre un punto determinado.

ii) Polvo
Se analizará el nivel de polvo que existe en el ambiente, este puede tener su origen en empresas cercanas, tales como serrerías, canteras, empresas dedicadas al cemento, etc. o bien en los elementos naturales que rodean la entidad, tales como grandes extensiones de arena, parques, etc.

iii) Incendios
Se debe analizar el riesgo de que se origine un incendio en los alrededores de la entidad que afecte a ésta. Principalmente se debe investigar que la actividad de las empresas cercanas, si emplean productos inflamables, si toman medidas de seguridad adecuadas, etc., así como la distancia del parque de bomberos más cercano.

iv) Interferencias
Es una amenaza que se debe analizar mediante dispositivos que nos permitan conocer el nivel de interferencias provenientes del exterior que se da en las instalaciones. Nos podemos fijar además en si existen grandes antenas cercanas, cables de alta tensión, etc.

c) Sociales

Se podrá hacer una pequeña investigación, principalmente acerca de posibles robos y actos de vandalismo que se hayan dado en la zona, así como de antecedentes de hurtos en edificios e instalaciones cercanas y en la propia entidad.

Realizar el cuestionario, entregar a las personas, que sirva para realizar la entrevista y para realizar las pruebas

4.3.4 - El personal

Como hemos comentado, una de las principales fuentes de información de las que vamos a disponer es el personal de la entidad. Las dos principales técnicas que vamos a emplear son el uso de cuestionarios y la realización de entrevistas personales. Hemos indicado ya los principales aspectos de estas dos técnicas en el capítulo anterior, por lo que no vamos a profundizar más en estos aspectos.

a) Cuestionarios

Como veremos en el capítulo siguiente, se les entregarán los cuestionarios a los empleados de la entidad auditada para que los rellenen, después los auditores deberán analizarlos y sacar las conclusiones correspondientes. Los cuestionarios deberán ajustarse para que los empleados que los realizan puedan contestar al máximo número de preguntas, por lo tanto se tendrá que tener presente la función o tareas que realizan éstos empleados y así adecuar el cuestionario.

b) Entrevistas

Del mismo modo, se emplearan las preguntas que han preparado en los cuestionarios para realizarlas en las entrevistas. Se deberá tener presente también las funciones y tareas que desarrolla el empleado al que se le va a realizar la entrevista, para escoger y adecuar las preguntas que se van a realizar.

4.3.5 - Revisiones y pruebas

Como ya hemos comentado, para verificar, comprobar y analizar la información que hemos ido recopilando, así como para aportar nuevos datos, es necesario realizar revisiones y pruebas de los sistemas a analizar. Una buena manera es seguir el cuestionario que hemos realizado, de esta manera no nos dejaremos ningún punto sin abordar.

Para la contestar a algunas preguntas del cuestionario, será necesario llevar a cabo una pequeña investigación. Por tanto, se deberán analizar todos los aspectos a tratar para planificar todas las comprobaciones y pruebas necesarias con antelación, probablemente en la fase de trabajo previo.

Como comentábamos al principio de este apartado, es muy importante realizar una buena observación. Mediante la observación podremos recopilar información que no vamos a conseguir de ninguna otra manera, por tanto, mientras que estemos realizando las pruebas y comprobaciones por las instalaciones, deberemos estar atentos para encontrar posibles deficiencias que se deban tener en cuenta.

4.3.6 - Fuentes externas a la entidad

Las fuentes externas a la entidad pueden aportar unos datos extras a nuestra investigación. En principio no va a haber muchas diferencias con los aspectos ya explicado en el capítulo anterior, por lo que tampoco profundizaremos demasiado en este aspecto.

Principalmente, deberemos investigar si las empresas instaladoras y mantenedoras de los sistemas que analicemos en el proceso de auditoría cumplen con los requisitos recomendados. Además podremos obtener información técnica acerca de los dispositivos instalados que la entidad auditada desconozca.

4.4 - Desarrollo del informe

En un proceso de auditoría informática de la Seguridad Física, los aspectos a tratar en el desarrollo del informe van a ser los mismos que para cualquier otro tipo de auditoría informática. Por tanto, se van a seguir los pasos y pautas comentadas en el capítulo anterior, no existiendo peculiaridades concretas para este caso.

Por tanto, se procederá al análisis de la información y se comprobará que se dispone de las evidencias suficientes. Si no se han conseguido, se deberán analizar los datos que nos faltan y volver a realizar las pruebas necesarias para obtenerlos. Una vez que se

dispone de la información necesaria, se procederá a encontrar las posibles deficiencias en la entidad y elaborar las recomendaciones correspondientes.

Se realizará un borrador del informe que se presentará a la entidad auditada para discutir los posibles errores y finalmente se realizará el informe definitivo, donde se incluirán todas las recomendaciones y aspectos relevantes.

5 - EL CUESTIONARIO

5.1 - Introducción

Como hemos anticipado en el capitulo anterior, he desarrollado un cuestionario general para emplear en una auditoría de la Seguridad Física. Lo he desarrollado siguiendo todos los aspectos que se han tratado en el capitulo 2 - Seguridad Física.

El cuestionario consta de una serie de preguntas, organizadas por temas. A su vez cada pregunta contempla una serie de posibles respuestas. Las preguntas y respuestas de la que consta este cuestionario se deberían adaptar dependiendo del objetivo, alcance y ámbito de cada auditoría en concreto, así como de las características específicas de la entidad auditada.

Las respuestas de las que consta cada pregunta están numeradas, por lo que para responder el cuestionario se deberá marcar con una X la columna que corresponda con el número de la respuesta. El número de respuestas posibles oscila entre 2 y 5, por lo que existen 5 columnas para marcar la respuesta que mejor refleje la realidad de la entidad auditada.

5.2 - Funcionamiento del cuestionario

Los temas en los que están organizadas las preguntas corresponden con las amenazas o factores los cuales pueden poner en peligro la Seguridad Física de la entidad, y se ha partido de la base de que existen una serie de factores que pueden hacer que el riesgo de que se produzca dicha amenaza sea mayor o menor, dependiendo de la entidad en concreto (situación geográfica, elementos cercanos, dispositivos internos, etc.). Por tanto, se contempla que el **riesgo para cada una de las amenazas va a ser variable**.

Por otro lado, existen una serie de **medidas que la entidad deberá adoptar para contrarrestar dichas amenazas**. Dependiendo del nivel de riesgo que se dé, se deberán tomar más o menos medidas de seguridad.

Para poder manejar toda esta información, se debe transformar en valores numéricos, de tal forma que:

i) Para cada amenaza se debe obtener un valor numérico. Se parte de un número que se va modificando con las respuestas obtenidas para las preguntas en ese bloque.

ii) Cuando se da la situación de equilibrio entre los riegos y las medidas de seguridad, el valor que se obtiene es 0.

iii) Cada amenaza en concreto parte de un valor que se le ha dado. Éste estará comprendido entre 0 y -5.

iv) Cada respuesta obtenida modificará ese valor. Si la respuesta se corresponde con una situación que hace que el riesgo aumente, le restará un coeficiente. Si por el contrario se

corresponde con una situación que hace que el riesgo disminuya, sumará un coeficiente. El coeficiente aplicado a cada respuesta es proporcional a la importancia que tiene.

v) Al final de cada bloque se obtendrá resultado. Cuanto mayor sea el resultado, más segura será la situación de la entidad ante esa determinada amenaza. Cuanto menor sea, mayor será el riesgo ante la amenaza. Si es menor que 0, estaremos hablando de una situación de riesgo, a la que se debe poner remedio. Si el resultado es mayor que 0, la amenaza está bien contrarrestada por las medidas de seguridad necesarias.

vi) Los coeficientes que hemos aplicado son variables. Es decir, dependiendo del objetivo, ámbito y profundidad de cada auditoría, se deberá dar más o menos importancia a cada aspecto, y por tanto, variar su coeficiente.

vii) Otro aspecto a tener en cuenta es que a raíz de las experiencias que se vayan obteniendo con este sistema, se deberán variar los coeficientes, para ajustarlos lo máximo posible a la realidad. Por tanto, la experiencia de los auditores es fundamental para obtener unos resultados verídicos.

viii) Se debe tener en cuenta que cada pregunta no analizará en sí un riesgo o un elemento de seguridad, si no que para una pregunta dada, una posible respuesta puede significar un riesgo (y restar un coeficiente), mientras que otra respuesta apunte a una medida de seguridad (y sume un coeficiente).

ix) El coeficiente de cada respuesta es independiente del número de respuesta de la pregunta. Es decir, para cada pregunta existen de 2 a 5 posibles respuestas numeradas del 1 al 5. Ese número sólo identifica la respuesta y el coeficiente dado depende de la importancia del factor analizado.

El coeficiente obtenido en cada tema solo nos va a decir si la entidad está expuesta o cubierta ante una determinada amenaza, y el grado en el que lo está. Por lo que al margen de todo esto, cada respuesta va a aportarnos información concreta acerca de los principales factores a tratar en un estad de Seguridad Física, por tanto un auditor deberá analizar todas las respuestas obtenidas para así averiguar donde están las posibles debilidades.

Para facilitar la comprensión del resultado obtenido, el coeficiente se puede expresar en **base 10**. De tal manera que se obtendrá un resultado desde 0 (el peor resultado posible) hasta 10 (el mejor), siendo 5 la posición de equilibrio. Para ello se debe conocer la nota mínima y máxima posible que se puede obtener y realizar un sencillo cálculo.

Por ejemplo, para el apartado de las copias de seguridad, la **nota mínima** que se puede obtener es -27 y la **nota máxima** 21. Una vez que se ha realizado el cuestionario, se obtendrá una **nota**. Para pasarla a base 10 se realizará lo siguiente:

i) Si la nota es igual a cero, la nota en base 10 será 5.

ii) Si la nota es menor que cero, la nota en base 10 se obtendrá de la siguiente operación:

$nota_{10}$ = 5 - (nota obtenida * (5 / nota mínima))

iii) Si la nota es mayor que cero, la nota en base 10 se obtendrá de la siguiente operación:

$nota_{10}$ = 5 + (nota obtenida * (5 / nota máxima))

Por tanto, si la nota en base 10 es menor que 5 existirán riesgos sin cubrir, y si es mayor que 5, todos los riesgos estarán cubiertos.

5.3 - Aplicaciones del cuestionario

El cuestionario va a ser la guía de los auditores a lo largo del desarrollo de la auditoría, ya que en éste están incluidos todos los aspectos y factores que se deben analizar para así poder concluir sobre el estado de la seguridad física de la entidad.

El cuestionario va a tener tres aplicaciones principales en el desarrollo de la auditoría, por un lado se lo podremos **entregar a los empleados** para que lo cumplimenten ellos mismos, por otro nos servirá como **batería de preguntas en las entrevistas** que hagamos, y por último, nos va a indicar todos los puntos y aspectos que se deberán verificar en el proceso de **pruebas y comprobaciones**. Vamos a ver en profundidad cada caso.

a) Cumplimentado por los empleados

Como ya hemos comentado en varias ocasiones, se podrá entregar una copia del cuestionario a los empleados que se crea conveniente para que lo cumplimenten. Para ello se ha desarrollado el cuestionario **Copia para los auditados**, en el cual se han suprimido los pesos de las respuestas para que, en principio, lo contesten más objetivamente. Se ha desarrollado también una **Tabla de pesos**, la cual utilizarán los auditores para obtener los resultados de los cuestionarios cumplimentados por los auditados.

b) En las entrevistas

Al realizar cada una de las entrevistas, el auditor podrá utilizar el cuestionario como batería de preguntas para realizar al entrevistado. Para ello utilizará la **Copia para el auditor**, dado que el auditor va a ser quien maneje el cuestionario, no se han eliminado los pesos de las respuestas, para que así pueda ir poniendo los resultados directamente en la columna correspondiente y ahorrándose de esta manera el proceso de comprobar el valor de cada respuesta con la tabla de pesos.

c) En pruebas y comprobaciones

Los auditores podrán utilizar el cuestionario como una guía para realizar todas las pruebas y comprobaciones oportunas. Según se vayan realizando estas pruebas, se irán anotando las respuestas en el cuestionario (Copia para el auditor), para así obtener directamente los resultados.

5.4 - Cuestionarios

Como ya hemos comentado, existen tres documentos para el cuestionario, la copia para los auditores, la copia para los auditados y la tabla de pesos. Los encontraremos en los **anexos 1, 2 y 3** de este trabajo respectivamente.

a) La copia para los auditores

Como hemos comentado, en la copia para los auditores se incluyen los pesos de las respuestas para así facilitar el trabajo. Para contestar a una pregunta, marcará una X en el número correspondiente a la respuesta y anotará el valor de ésta en la columna **Valor**.

b) La copia para los auditados

Como ya hemos comentado, en la copia para los auditados se ha suprimido el valor de cada pregunta, de esta manera los empleados que contesten al cuestionario lo harán objetivamente, ya que, en principio, no saben si van a obtener unos buenos o malos resultados en función de las respuestas. Lógicamente, pueden intuir si las respuestas que den van a van a ofrecer una buena o mala imagen de la entidad, por tanto puede que mientan o no se ajusten a la realidad. Es por ello que se deben realizar todas las comprobaciones que se crean necesarias.

c) La tabla de pesos

La tabla de pesos simplemente asigna un peso a cada pregunta. Se he realizado para facilitar el trabajo de los auditores a la hora de revisar los cuestionarios contestados por los empleados. Como hemos comentado, los pesos de cada respuesta pueden variar dependiendo de la auditoría en concreto, así como de las experiencias de los auditores, por ello se debe tener en cuenta que cuando se cambien los pesos se deberán cambiar tanto en la tabla de pesos como en la copia para los auditores, donde se han incluido los pesos para facilitar el trabajo.

6 - LA APLICACIÓN

6.1 - Introducción

Para facilitar la labor de los auditores, se ha desarrollado para este trabajo una **aplicación informática**. Ésta se ha elaborado con ***Microsoft® Visual Basic 6.0***, ya que permite crear fácilmente un interfaz gráfico intuitivo y agradable. Básicamente, la aplicación permite realizar el cuestionario de una manera más cómoda, ofreciendo los resultados del mismo de manera inmediata, así como recomendaciones para aumentar la seguridad en función de los resultados obtenidos. Por ser un **prototipo**, sólo está implementado el apartado de las copias de seguridad. Vamos a ver todos estos aspectos en profundidad.

Durante el desarrollo de la auditoría se podrá emplear la aplicación para que los empleados realicen el cuestionario o para que los auditores introduzcan los datos directamente mientras realizan las pruebas y comprobaciones necesarias. También se pueden recopilar todos estos datos en papel, empleando el cuestionario, y después introducir la información obtenida en la aplicación, para que así nos muestre los resultados y posibles recomendaciones rápidamente.

6.2 - Características de la aplicación

Aunque, como hemos comentado, la aplicación permite realizar el cuestionario de una manera más cómoda, existen algunas peculiaridades que se deben comentar.

i) Las cuestiones

Las cuestiones que se han incluido en la aplicación son las mismas que las del cuestionario. Tienen las mismas respuestas y cada una de éstas tiene el mismo coeficiente.

ii) Eliminación dinámica de cuestiones innecesarias

En el cuestionario no se pueden eliminar cuestiones en función de las respuestas que se han ido obteniendo. Sin embargo, en la aplicación esto sí se puede hacer. Si por ejemplo, una cuestión pregunta si *existe una política de realización de copias de seguridad* y la respuesta es *no*, no será necesario preguntar después si la política se sigue.

Para que en el cuestionario conteste a la pregunta de si se sigue, se ha incluido la respuesta de *no existe un política…* con un coeficiente igual a cero, por lo que, en cierto modo, está respondiendo dos veces a lo mismo. Sin embargo, en la aplicación, si la respuesta a la pregunta de si *existe una política de realización de copias de seguridad* es no, *no* se realizarán preguntas referentes a ésta, si no que se pasará a la siguiente. Si por el contrario es *sí*, al cuando preguntemos si ésta se sigue, no aparecerá la respuesta de que no existe.

iii) Recomendaciones

En la aplicación se han incluido una serie de recomendaciones. Éstas dependerán de las respuestas que se den para cada pregunta. Un vez que se hayan respondido todas las cuestiones, la aplicación habrá seleccionado las recomendaciones adecuadas de todas las que contempla. Puesto que no todas preguntas tienen la misma importancia (no es lo mismo que no exista una política de ahorro de tiempo de copiado a que no se realicen copias de seguridad), las recomendaciones tampoco serán igual de importantes.

Para ello se ha creado el **grado de importancia o criticidad**. Éste es una característica de cada recomendación en concreto y depende de la importancia de la medida que se debe adoptar. El grado de importancia está comprendido entre 0 (la recomendación es muy poco importante) hasta 10 (es muy importante que se tomen medidas y se siga la recomendación dada). Cuando se muestran las recomendaciones están ordenadas y agrupadas según su grado de importancia, de más importante a menos importante.

Lógicamente, las recomendaciones que se den finalmente a los auditados, dependerán de la entidad en concreto, del objetivo, ámbito y profundidad de la auditoría y de la experiencia y criterio de los auditores.

iv) Resultados

Como hemos comentado, la aplicación va a ofrecer de manera inmediata unos resultados al finalizar el cuestionario. En estos se ha incluido **la nota obtenida**, que estará comprendida entre la nota máxima y la nota mínima, que también se muestran para que el usuario se haga una idea de la situación. También se muestra la **nota obtenida en base 10**, ya que, como hemos comentado, es mucho más fácil de comprender. Para obtener la nota en base 10 se realizan las operaciones que hemos comentado en el capítulo 5 - El cuestionario.

Además, y dependiendo de la nota en base 10 que se haya obtenido, se muestra la **situación de la entidad**, esta puede ser muy buena, si la nota en base 10 es mayor 8, buena, si la nota es igual a 7 o a 8, delicada, si la nota obtenida es igual a 5 o a 6, mala, si la nota es igual a 3 o a 4 o muy mala, si la nota es menor que 3. Además se ha añadido un comentario aclaratorio que define brevemente cada una de las posibles situaciones.

6.3 - Manejo de la aplicación

La aplicación está diseñada para el sistema operativo ***Windows*** en todas sus versiones. Para comenzar basta con hacer doble-clic en el archivo ejecutable. Se muestra la ventana de bienvenida (imagen 1), donde podremos presionar *salir* para abandonar el programa o *continuar* para comenzar.

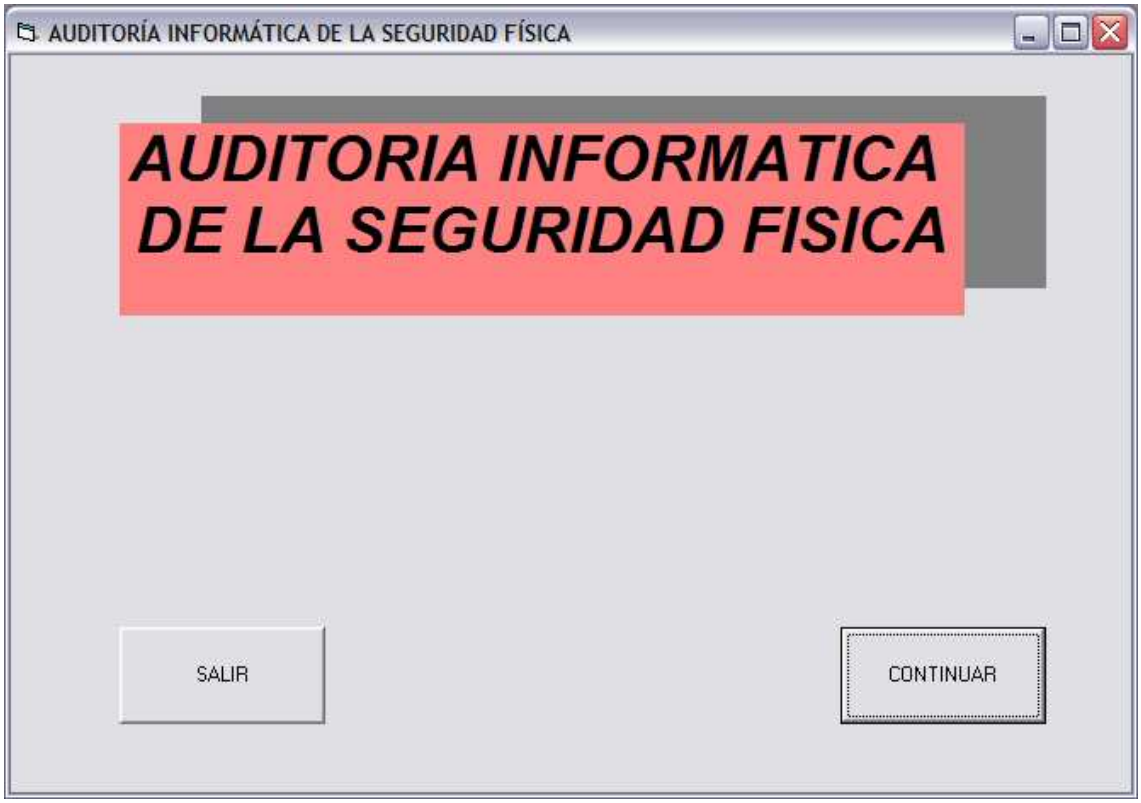


Imagen 1

Al presionar el botón *continuar* se muestra una pantalla donde se escogerá la categoría sobre la que se desea realizar el cuestionario (imagen 2). Presionando sobre el botón correspondiente se accederá al cuestionario seleccionado. Recordemos que en este caso solo está implementada la opción *Copias de seguridad*.

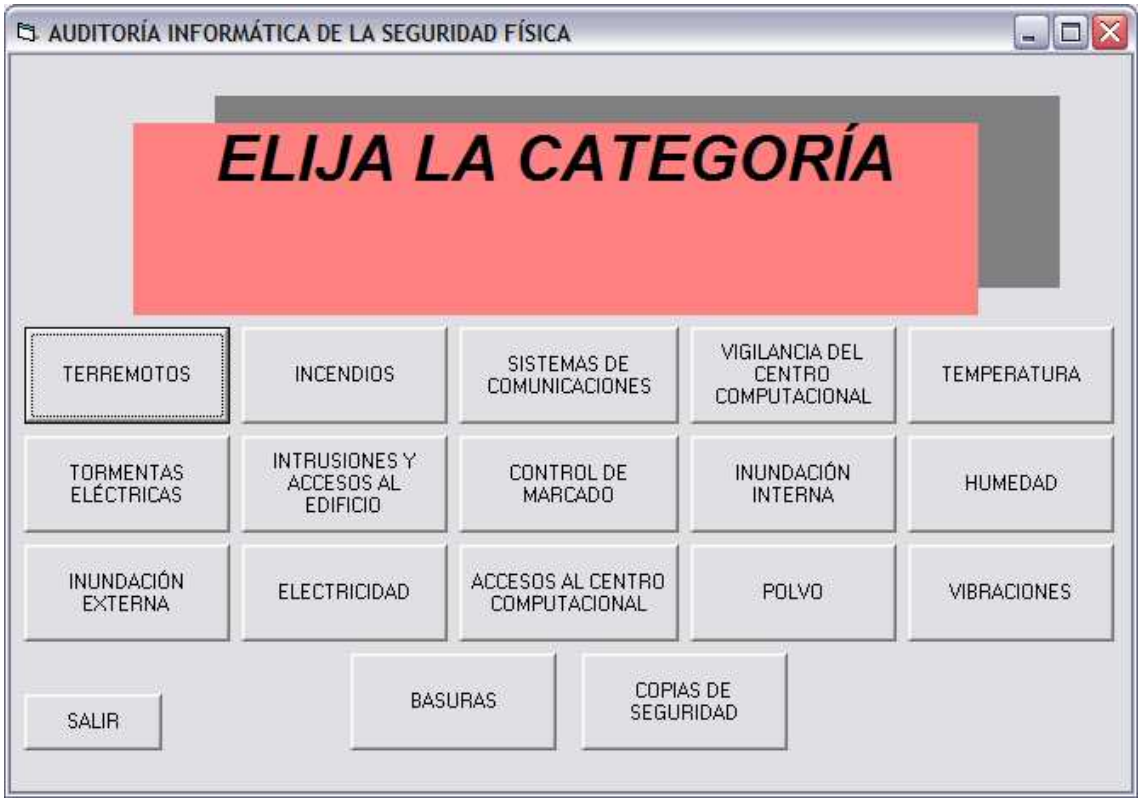


Imagen 2

Al presionar sobre el botón de una da las categorías, se abrirá la ventana de bienvenida de la categoría (imagen 3), en nuestro caso presionamos *Copias de seguridad*.

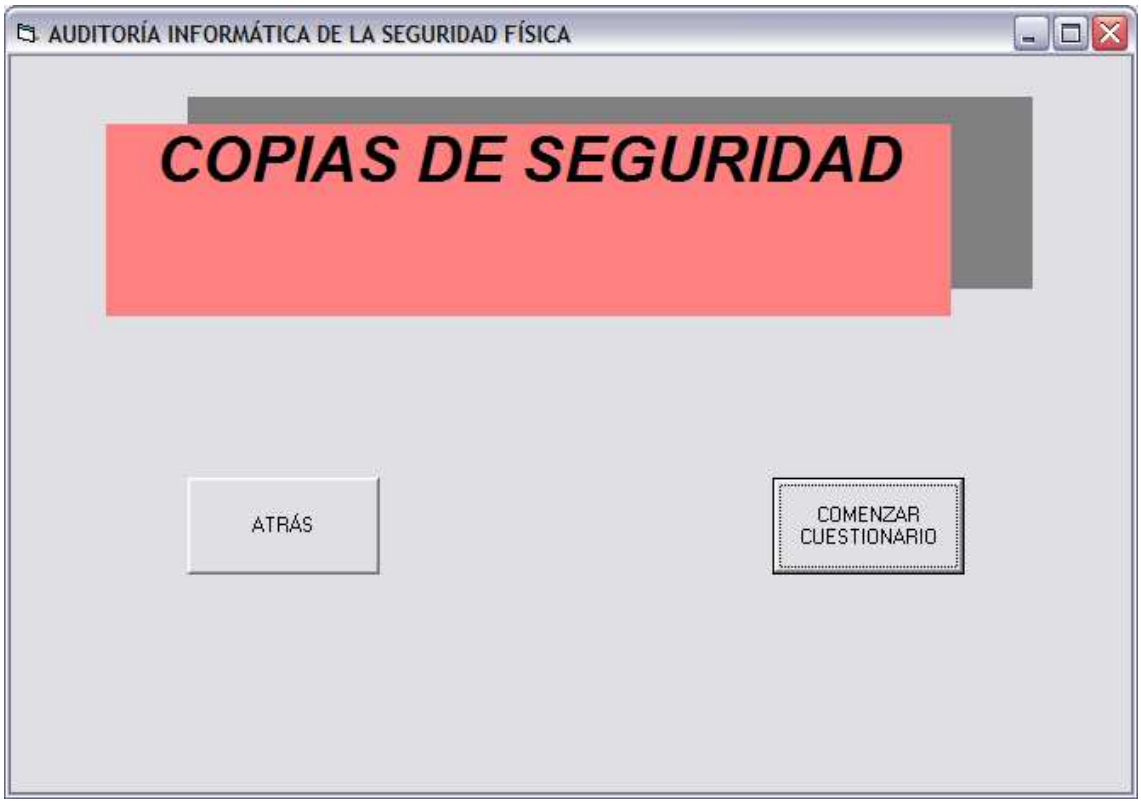


Imagen 3

En este punto, el usuario tiene dos opciones, presionar el botón *atrás*, volviendo a la selección de categoría (imagen 2) o presionar el botón de *comenzar cuestionario*, con lo que se abrirá la ventada con la primera pregunta (imagen 4).

En esta imagen se pueden apreciar varios elementos: lo primero que nos encontramos es el ámbito al que hace referencia la pregunta (1). En el caso de las copias de seguridad éste podrá ser *ámbito general*, referido a las *copias y sistemas de copias en línea* y referido a las *copias y sistemas de copias fuera de línea*. El siguiente elemento es el número de la cuestión que se está proponiendo (2). Más abajo nos encontramos con la pregunta (3) y las respuestas (4). El sistema de selección de las preguntas es el de *check-box*, esto es, el usuario sólo podrá marcar una respuesta de todas las posibles. Una vez que se ha marcado la respuesta correspondiente, se presiona el botón *validar* (5) para pasar a la siguiente pregunta.

Éste funcionamiento es el mismo para todas las preguntas del cuestionario, hasta que se llega a la última (imagen 5), donde se presionará el botón *validar y ver resultados* para acceder a la pantalla de resultados (imagen 6).

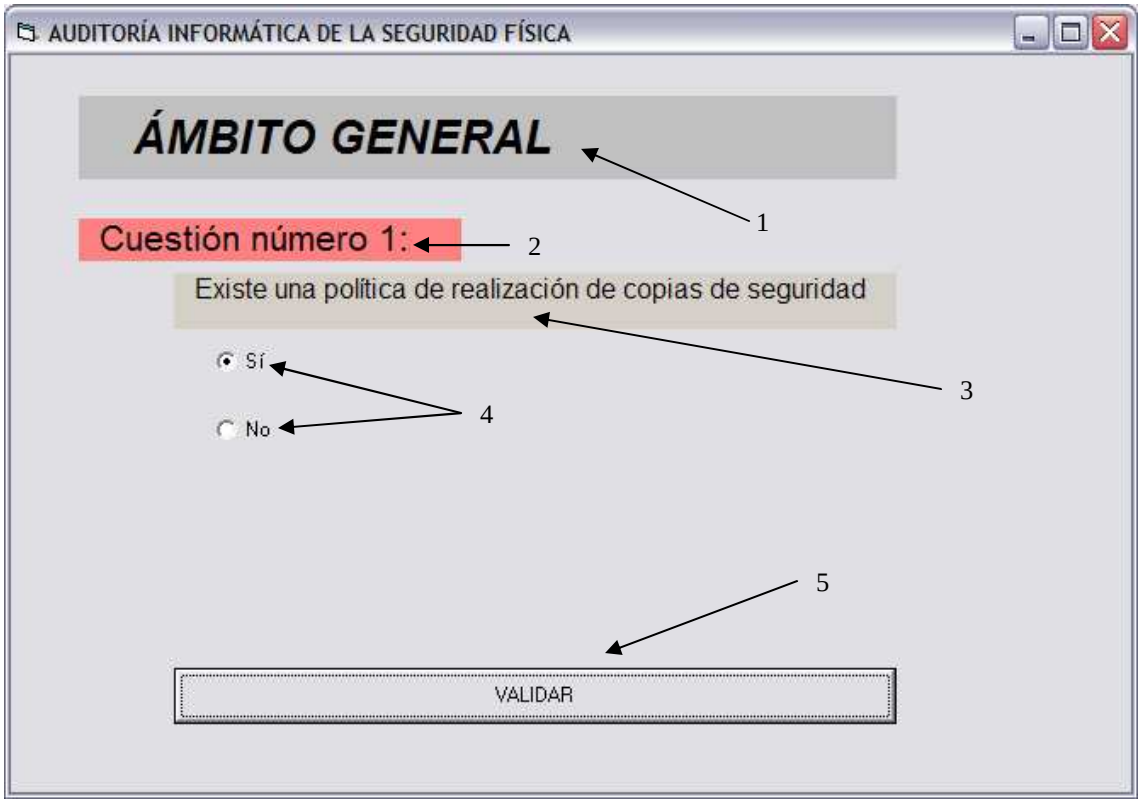


Imagen 4

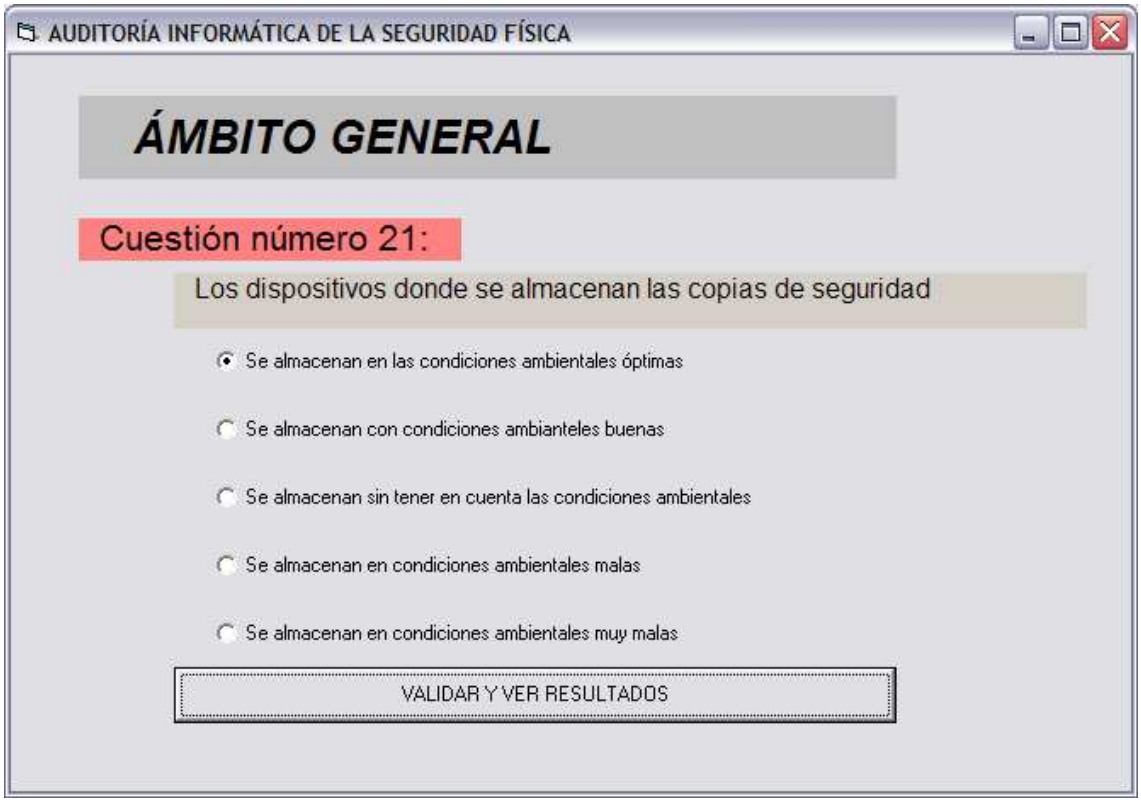


Imagen 5

En la pantalla de resultados se muestra el coeficiente obtenido (1) que estará comprendido entre el coeficiente máximo y el coeficiente mínimo de la categoría (2), la nota obtenida en base 10 (3), que será de 0 a 10 y la situación de la entidad (4), que podrá ser muy buena, buena, delicada, mala y muy mala.

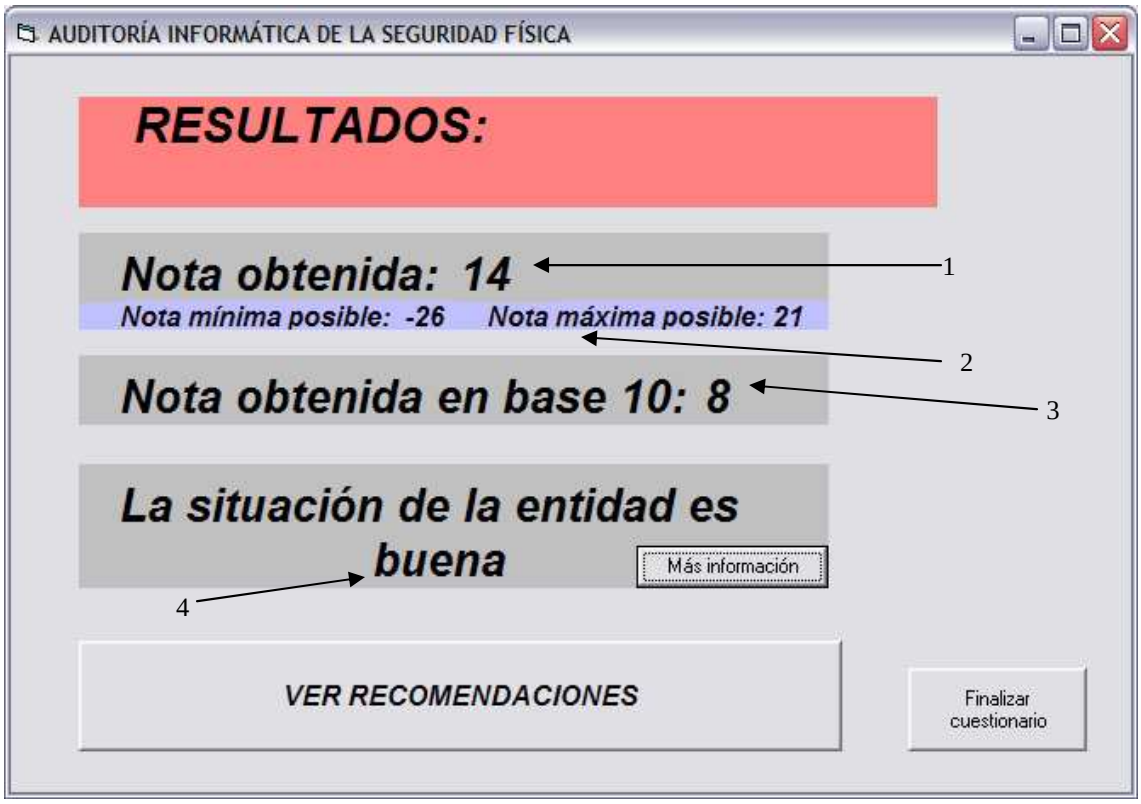


Imagen 6

Presionando el botón de *más información* se abrirá una ventana (imagen 7) donde podremos obtener un pequeño comentario acerca de la situación general en la que se encuentra la entidad sobre la categoría seleccionada. Presionando *volver* se cerrará esta ventana.

Si se presiona el botón de *ver recomendaciones*, se mostrarán las recomendaciones que se deben dar en función de las respuestas obtenidas (imagen 8). Las recomendaciones están agrupadas y ordenadas por el nivel de criticidad de cada una, mostrándose primero las más importantes y al final las menos importantes. Al igual que la anterior, esta ventana se cerrará presionando el botón *volver*.

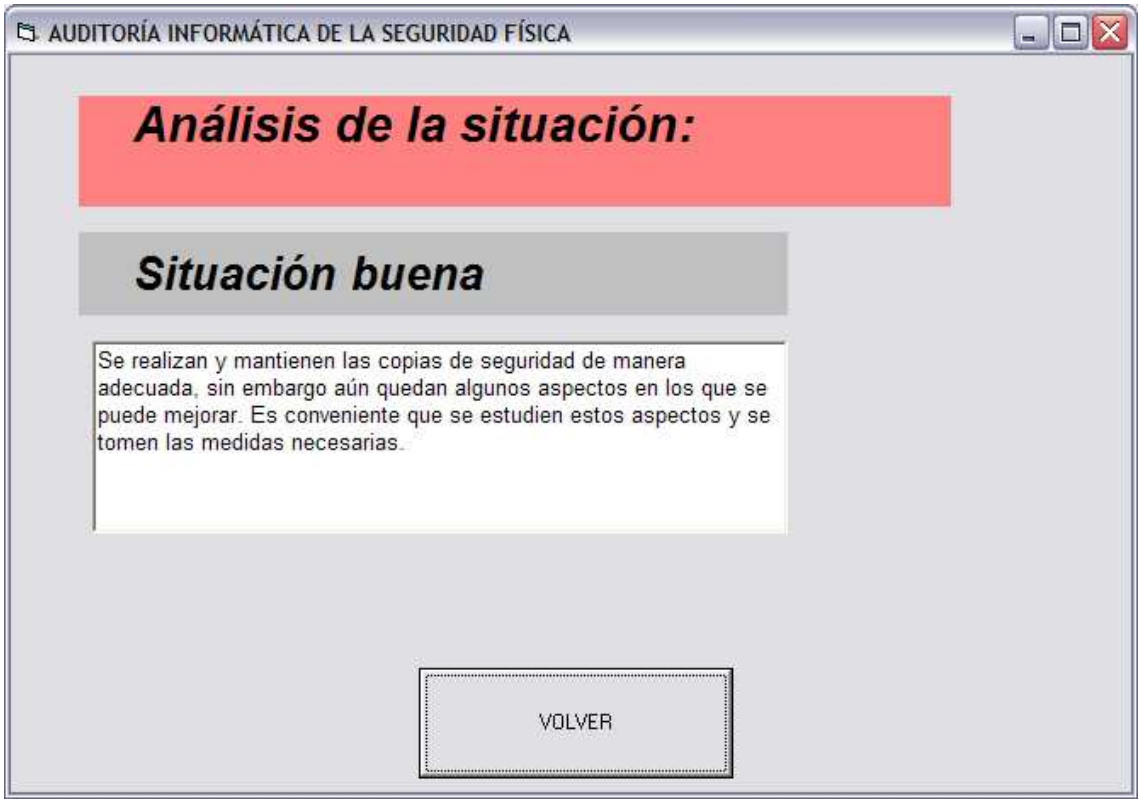


Imagen 7

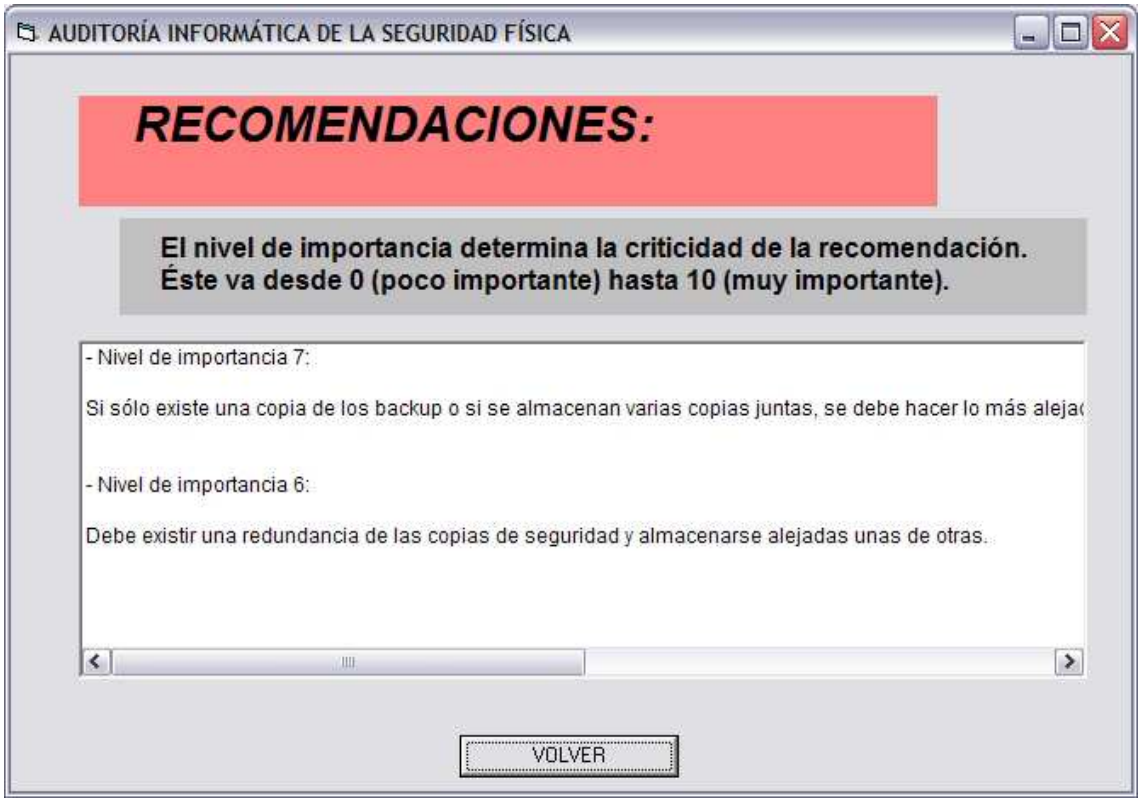


Imagen 8

Cuando nos encontremos de nuevo en la pantalla de resultamos (imagen 6), podremos presionar el botón *finalizar cuestionario*, con lo que se borrarán de la memoria toda la información recopilada y se volverá a la pantalla de selección de categoría (imagen 2), donde podremos realizar otro cuestionario o salir de la aplicación, mostrándose por tanto la pantalla de despedida (imagen 9). Presionando el botón salir se cerrará por completo la aplicación.

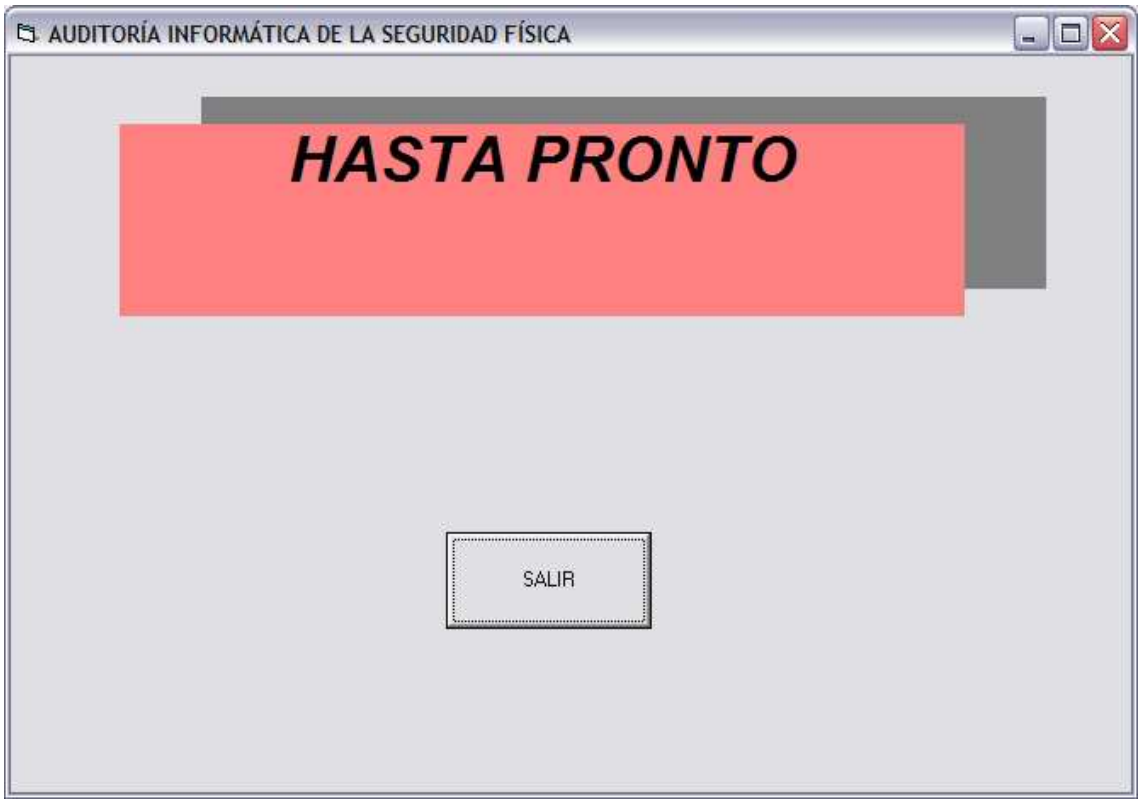


Imagen 9

7 - CASO PRÁCTICO

7.1 - Introducción

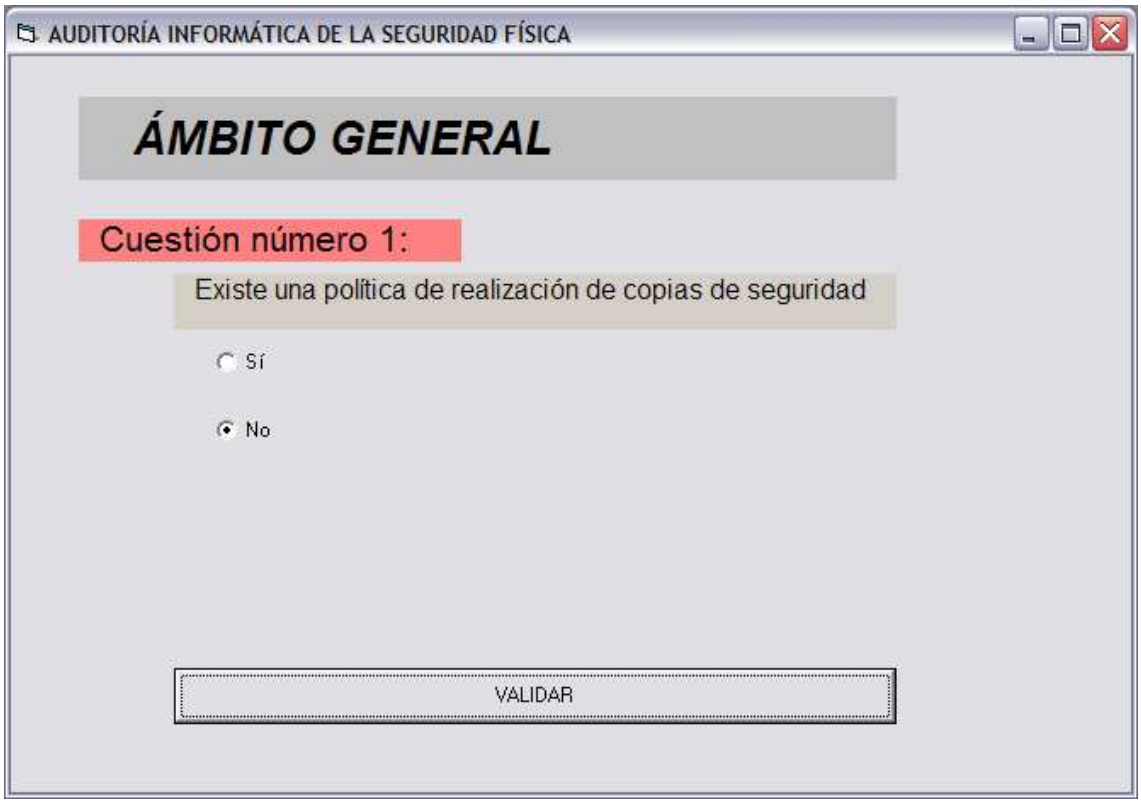
Para ver de manera explicita el funcionamiento de la aplicación informática, vamos a ver dos casos prácticos. Vamos a partir de una situación imaginaria y concreta con respecto a la gestión y seguridad de los backups, ejecutaremos la aplicación e iremos contestando a las preguntas con las respuestas correspondientes en cada caso, para mostrar los resultados obtenidos y las recomendaciones dadas.

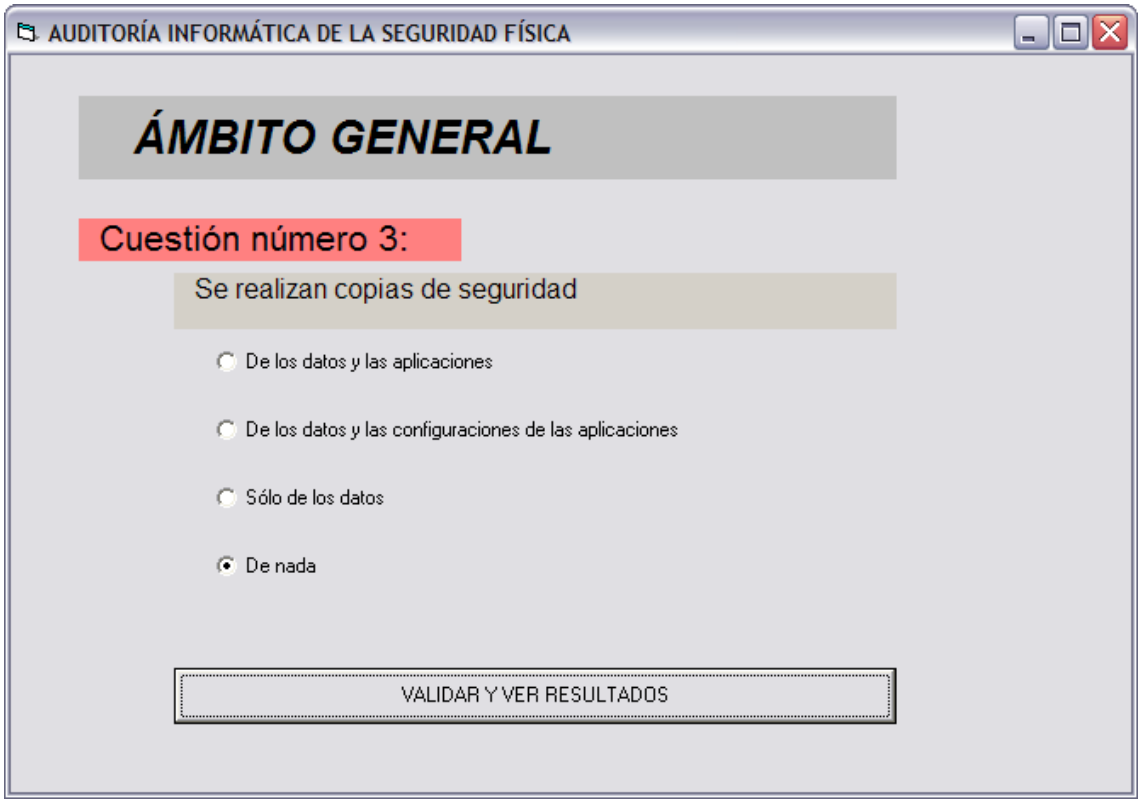
7.2 - Caso práctico 1

a) Situación de la entidad

La entidad es una empresa que solamente almacena información de sus clientes, proveedores y empleados. Sólo las se almacenan en un servidor al cual se puede acceder desde varios puntos de las instalaciones. No se realizan copias de seguridad de nada y no se ha estudiado si quiera la posibilidad de hacerlo, ya que no se considera importante.

b) Respondiendo al cuestionario

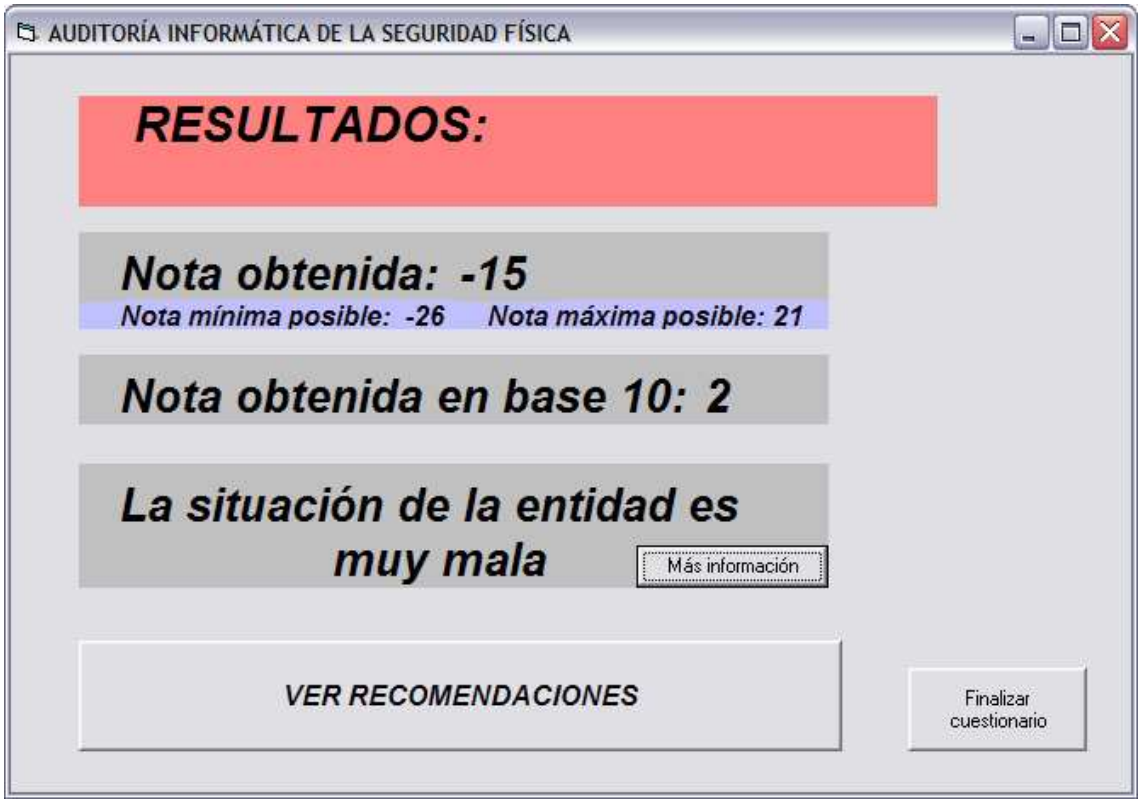


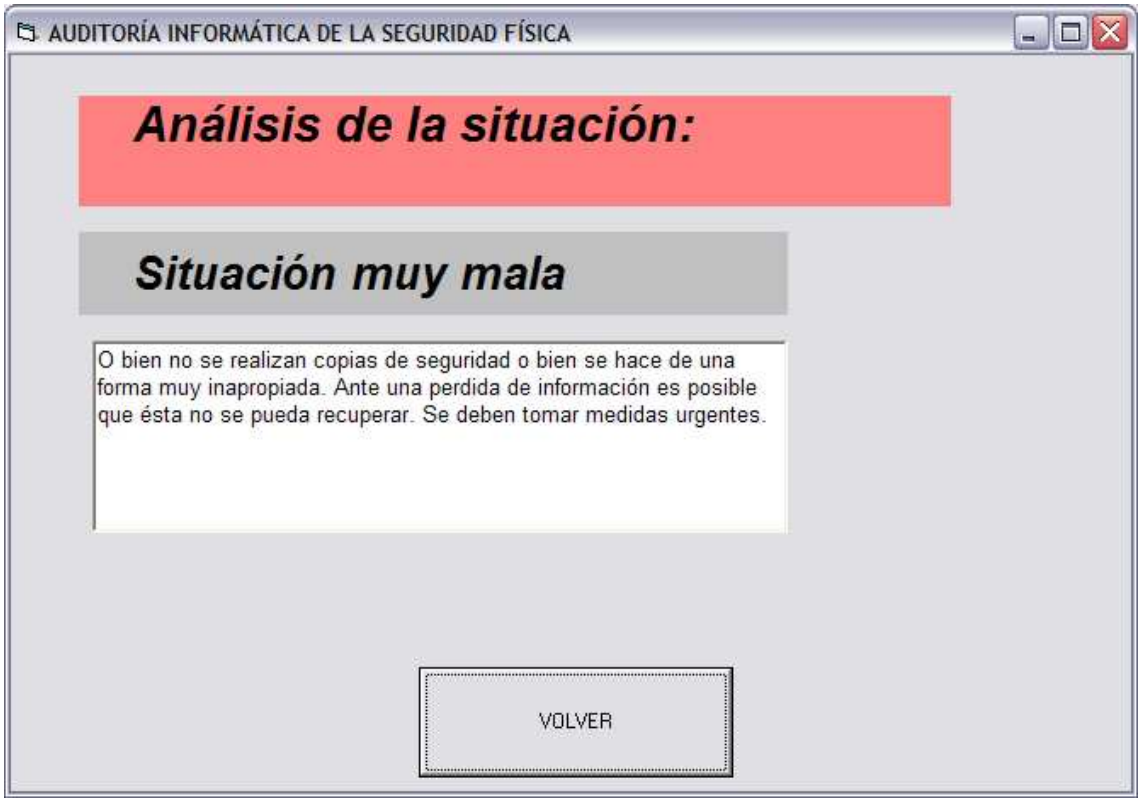


Como ni existe una política de realización de copias de seguridad ni se hacen copias de seguridad de nada, no tiene sentido seguir preguntando por los sistemas en concreto, por lo que finalizará el cuestionario.

c) Resultados

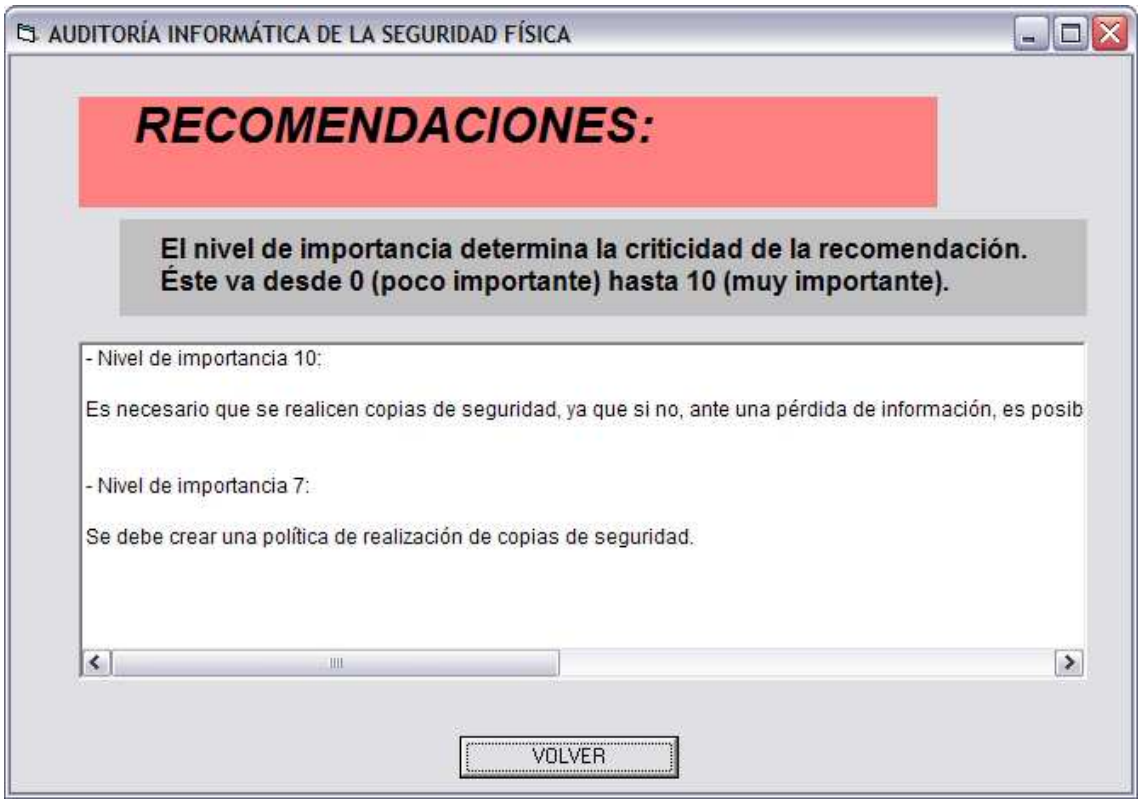
A continuación vamos a mostrar la pantalla de resultados. En principio podría parecer que por no realizar copias de seguridad de nada debería haber obtenido la peor nota posible. Sin embargo y como veremos a continuación, esto no es así, ya que una entidad que realizara copias de seguridad pero que éstas no sean válidas a la hora de restaurar el sistema o que se almacenan de tal manera que un intruso las pudiera sustraer o copiar, consiguiendo de ésta manera toda la información de la entidad, estaría corriendo aún un riesgo mayor.


AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
RESULTADOS:
Nota obtenida: -15
Nota mínima posible: -26
Nota máxima posible: 21
Nota obtenida en base 10: 2
La situación de la entidad es muy mala
Más información
VER RECOMENDACIONES
Finalizar cuestionario


AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
Análisis de la situación:
Situación muy mala
O bien no se realizan copias de seguridad o bien se hace de una forma muy inapropiada. Ante una perdida de información es posible que ésta no se pueda recuperar. Se deben tomar medidas urgentes.
VOLVER

d) Recomendaciones

Una vez que se han mostrado los resultados del cuestionario, vamos a ver las recomendaciones para este caso en concreto, que, obviamente, harán referencia a la creación de una política de copias de seguridad y la implantación de la misma.

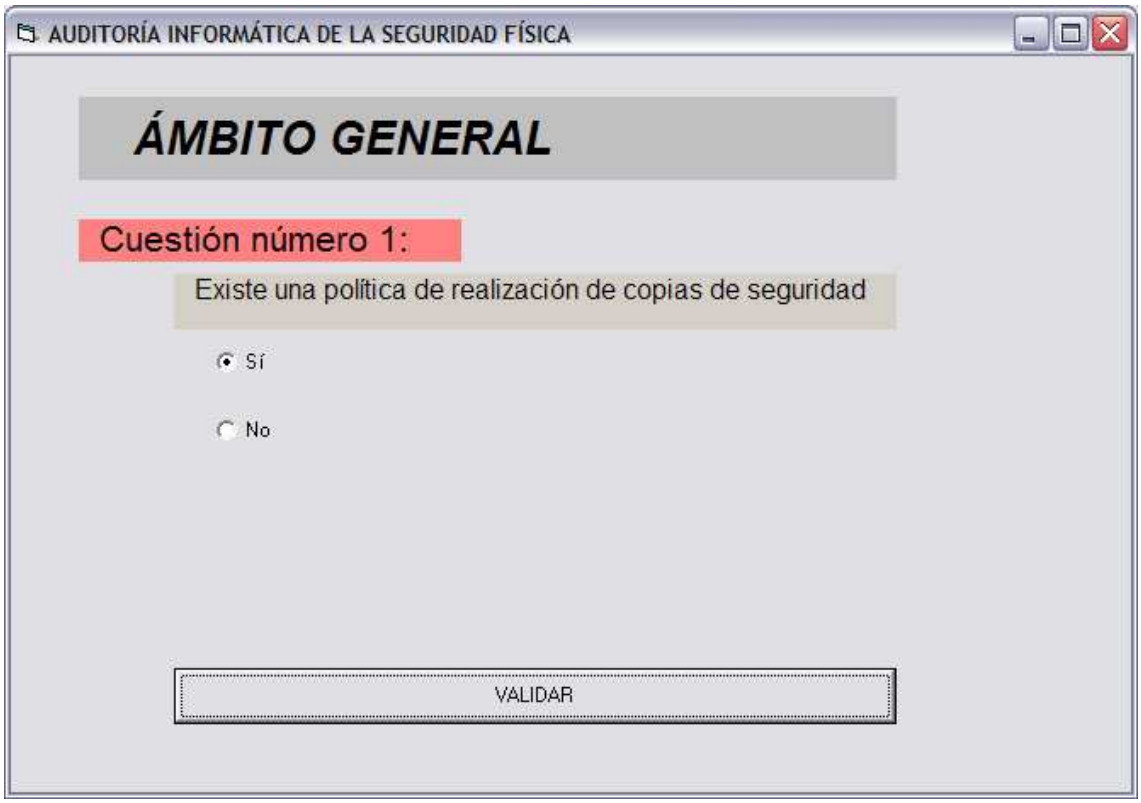


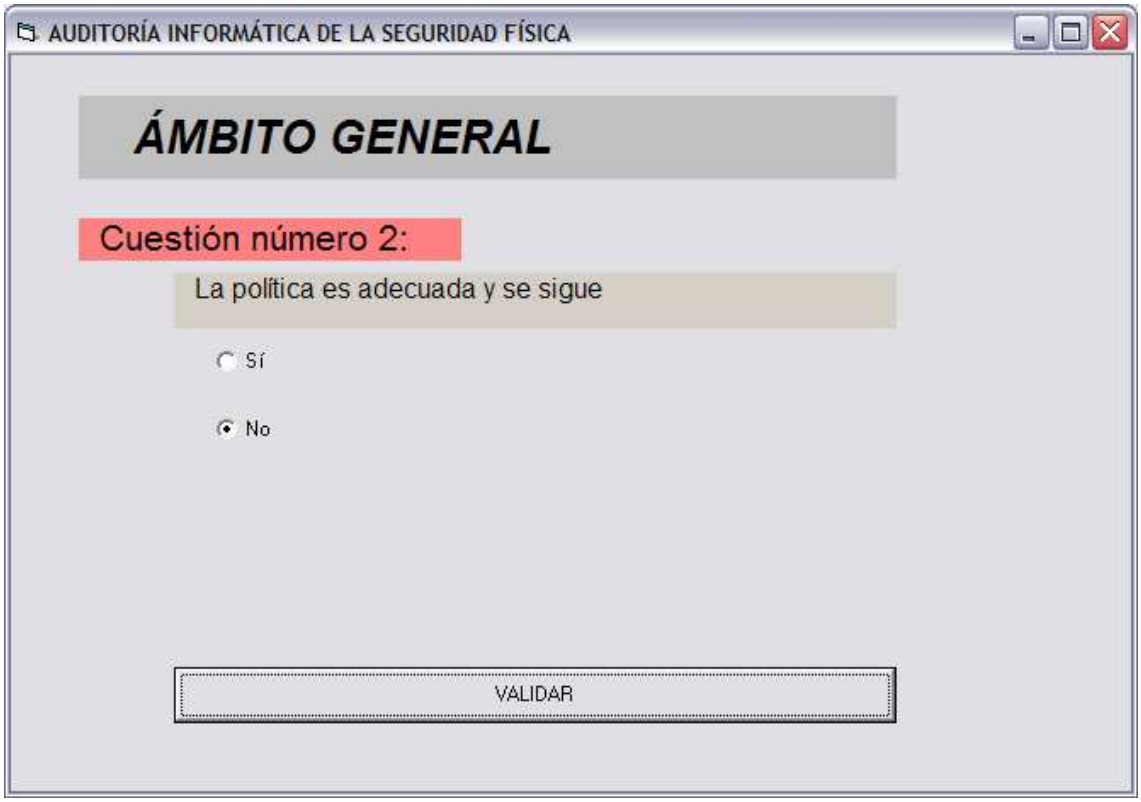
7.3 - Caso práctico 2

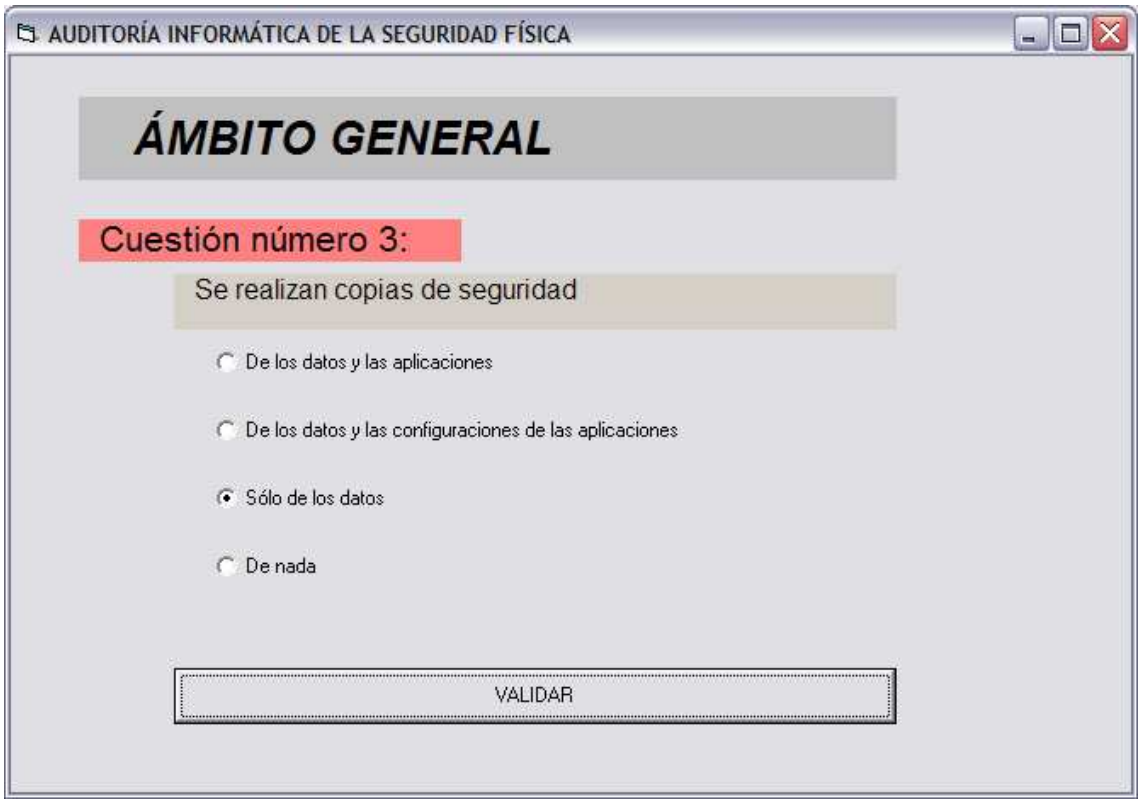
a) Situación de la entidad

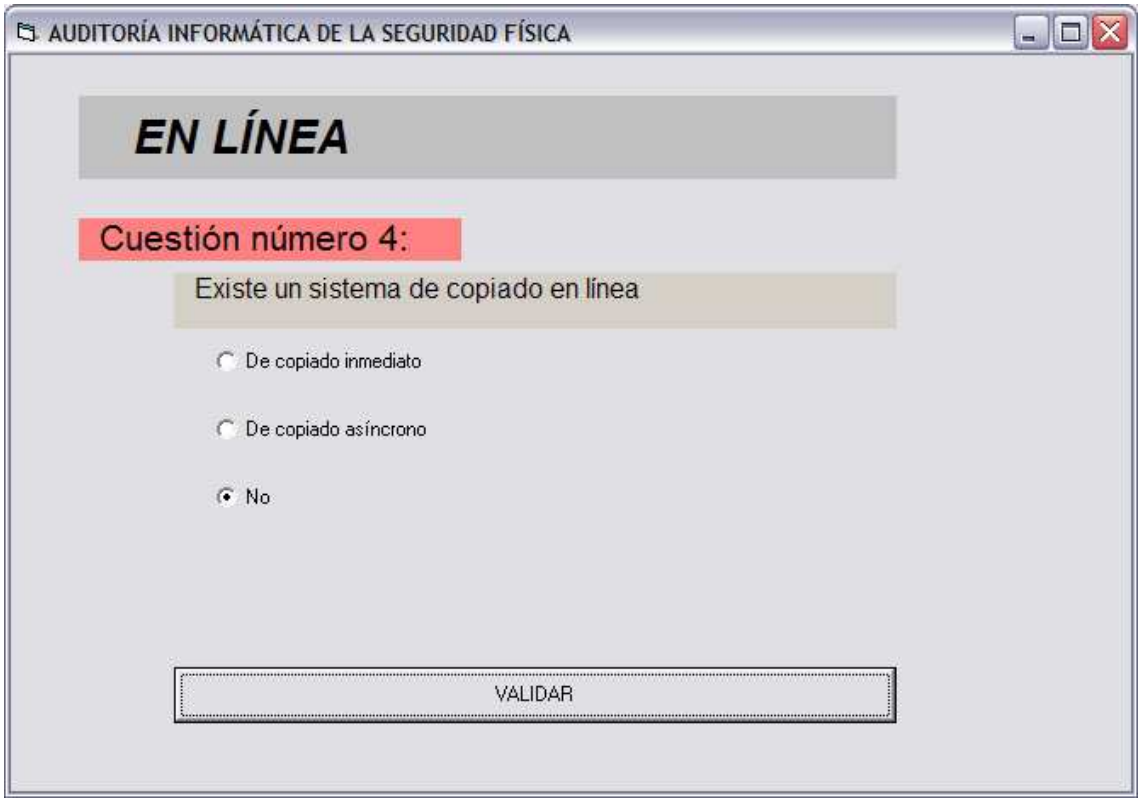
En este caso, la entidad en cuestión es una gran empresa, donde se da una gran importancia a la información almacenada por ser desarrollada por ellos mismos. Por lo tanto existe una política de realización de copias de seguridad adecuada, pero que sin embargo, no se sigue correctamente. Se realizan copias de seguridad sólo de los datos, puesto que se dispone de los originales de las aplicaciones en caso de que sea necesario restaurarlas. El sistema que se emplea para realizar las copias de seguridad es un sistema fuera de línea, considerado como crítico, empleando para ello cintas de backup. Como se realizan por la noche, no se ha estudiado ninguna técnica para reducir el tiempo de copiado. Se realiza una copia incremental, ya que los estudios dicen que es la más adecuada. Las cintas de backup se reutilizan y, aunque se ha estudiado la manera más adecuada de hacerlo, no se hace así. No existe redundancia de las copias de seguridad y éstas se almacenan en otro edificio de la entidad, guardadas en una caja fuerte donde da directamente el sol, por lo que la temperatura que se alcanza es muy elevada, superior a la recomendada por los fabricantes de las cintas. Se hizo una restauración del sistema de prueba hace años.

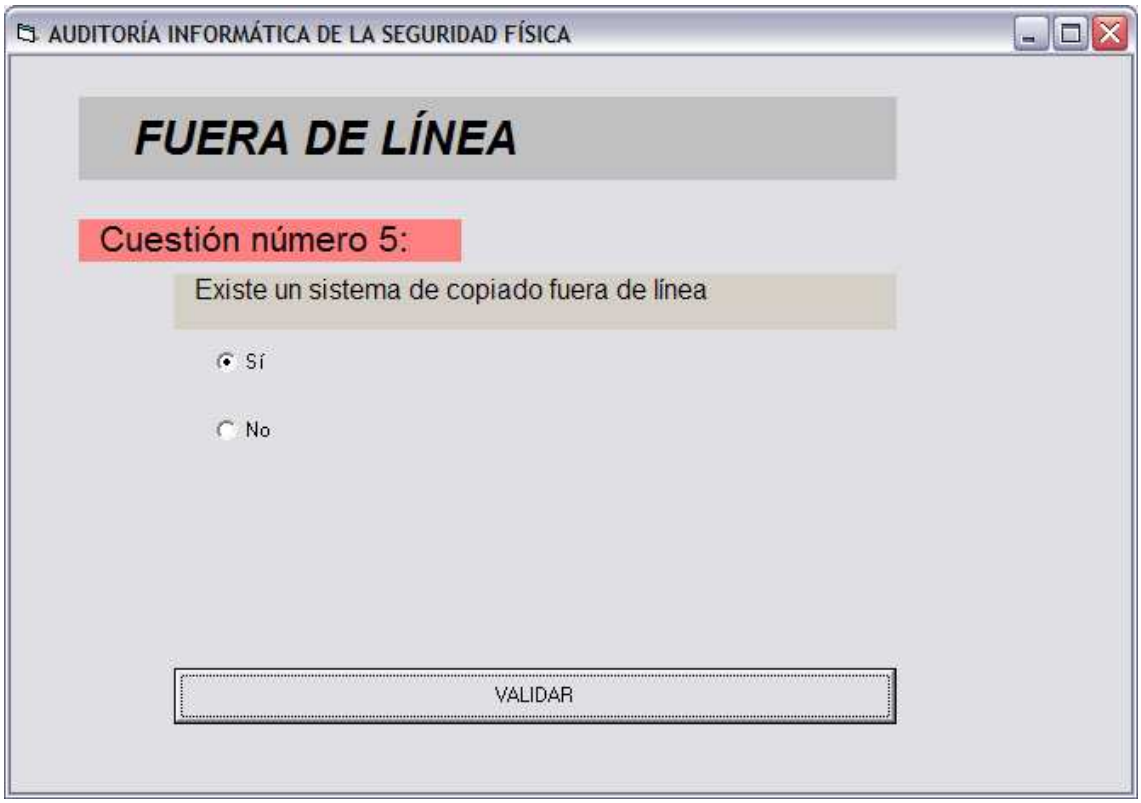
b) Respondiendo al cuestionario

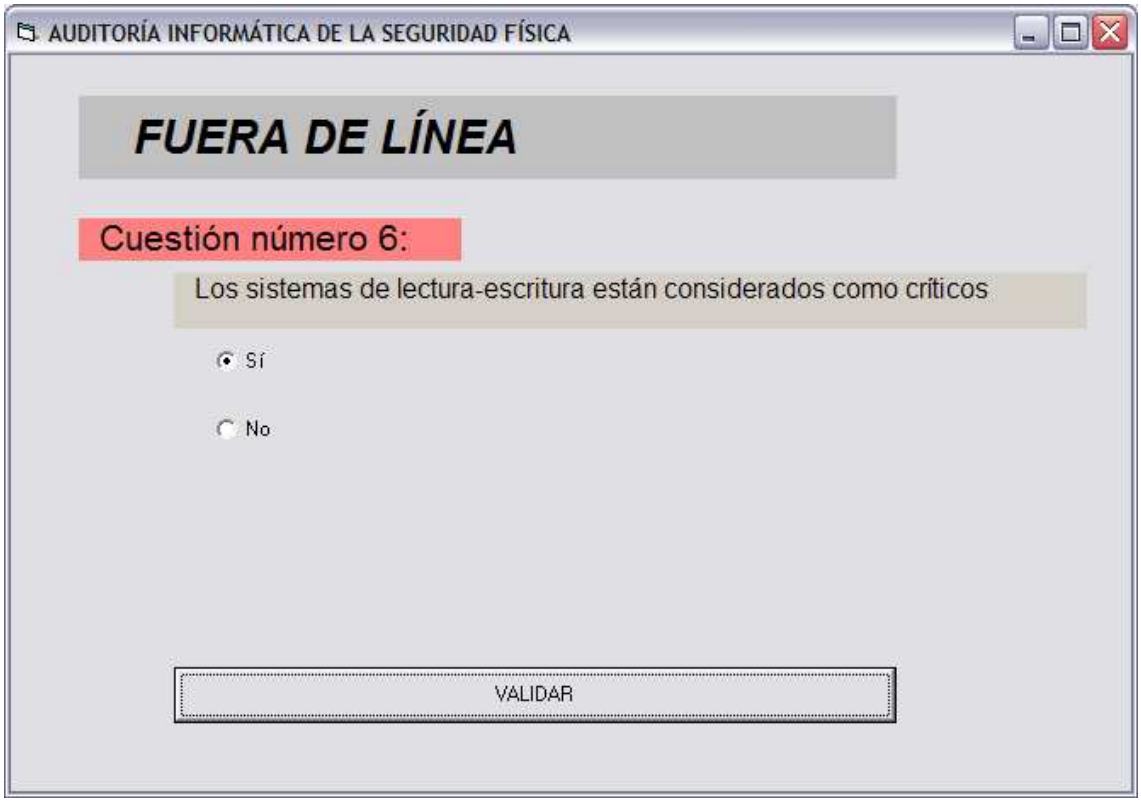


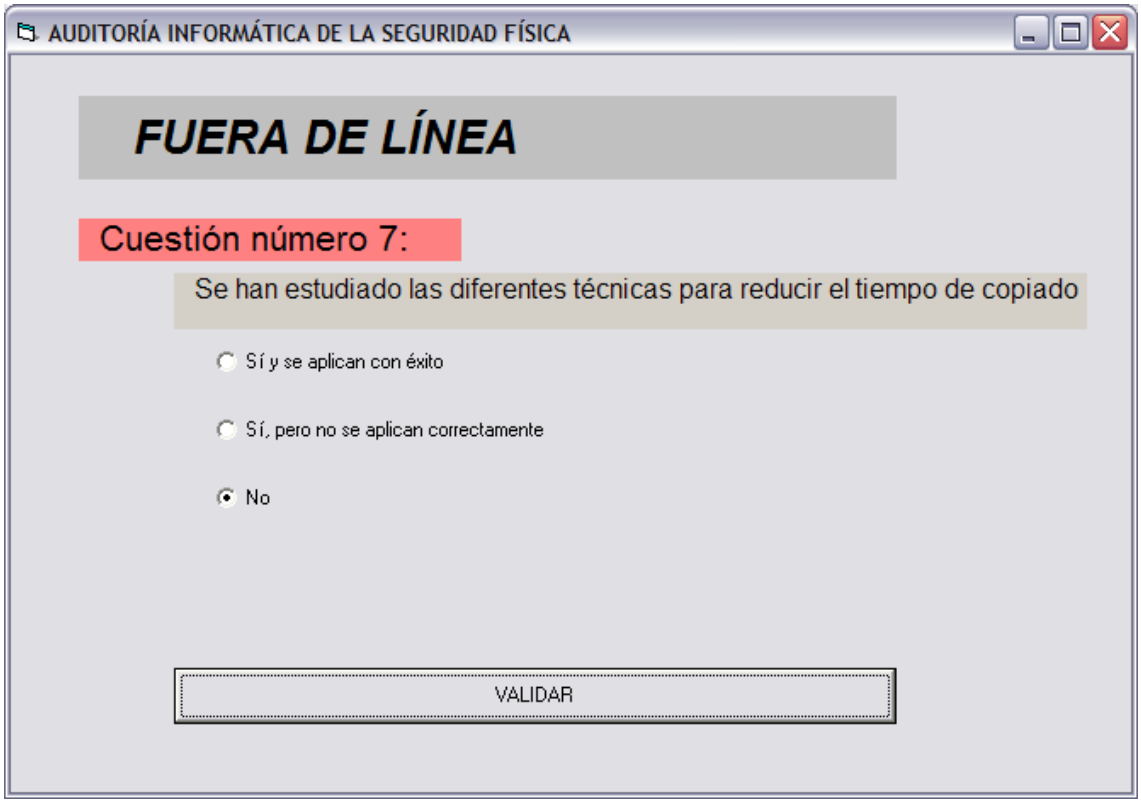


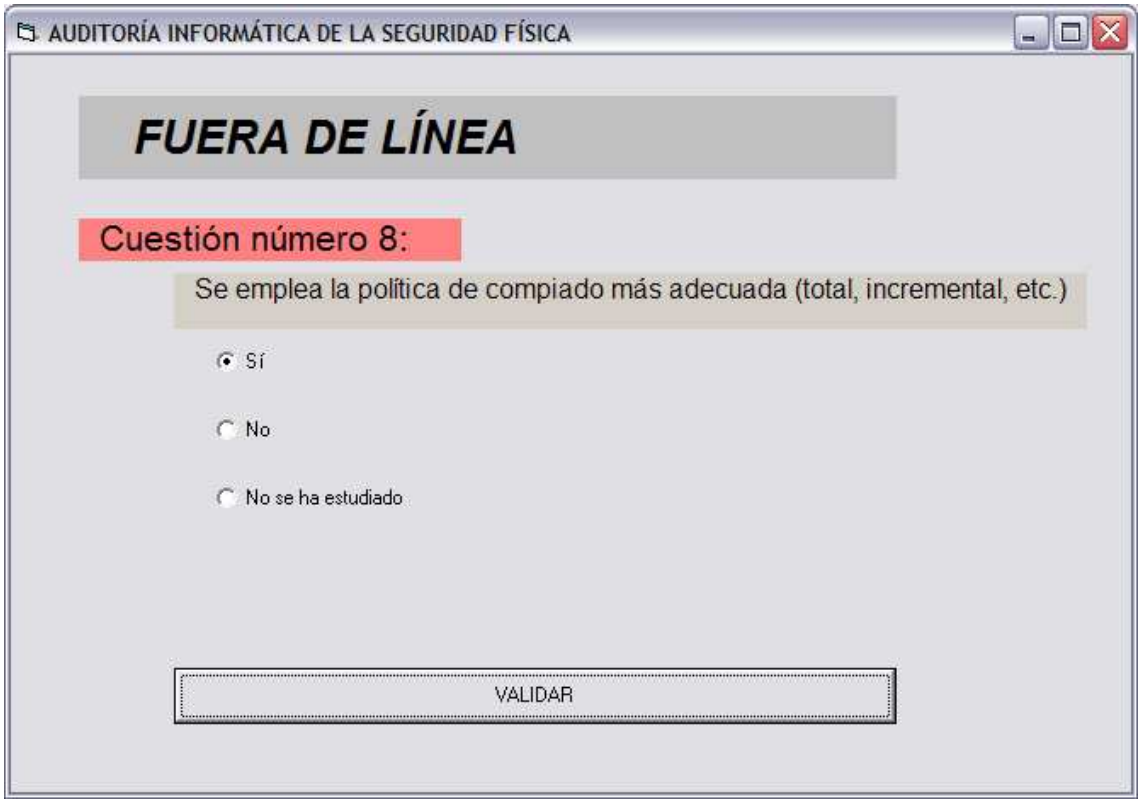

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
ÁMBITO GENERAL
Cuestión número 3:
Se realizan copias de seguridad
De los datos y las aplicaciones
De los datos y las configuraciones de las aplicaciones
Sólo de los datos
De nada
VALIDAR

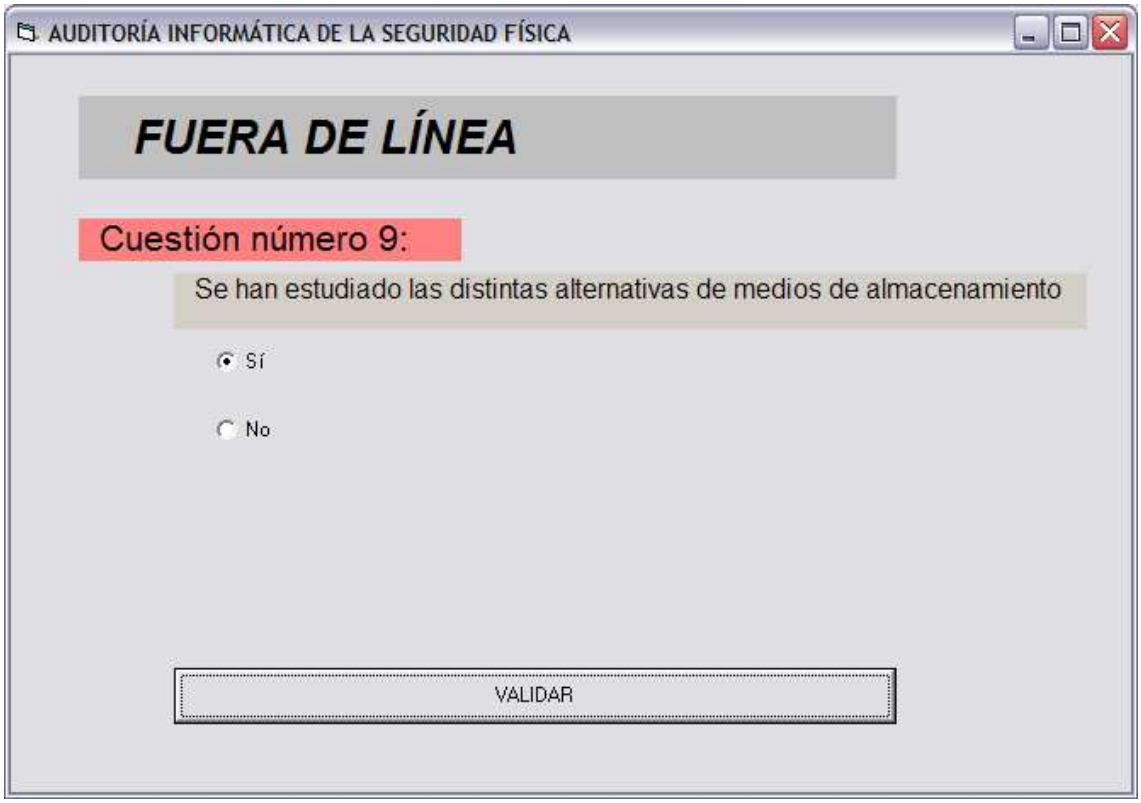

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
EN LÍNEA
Cuestión número 4:
Existe un sistema de copiado en línea
De copiado inmediato
De copiado asíncrono
No
VALIDAR

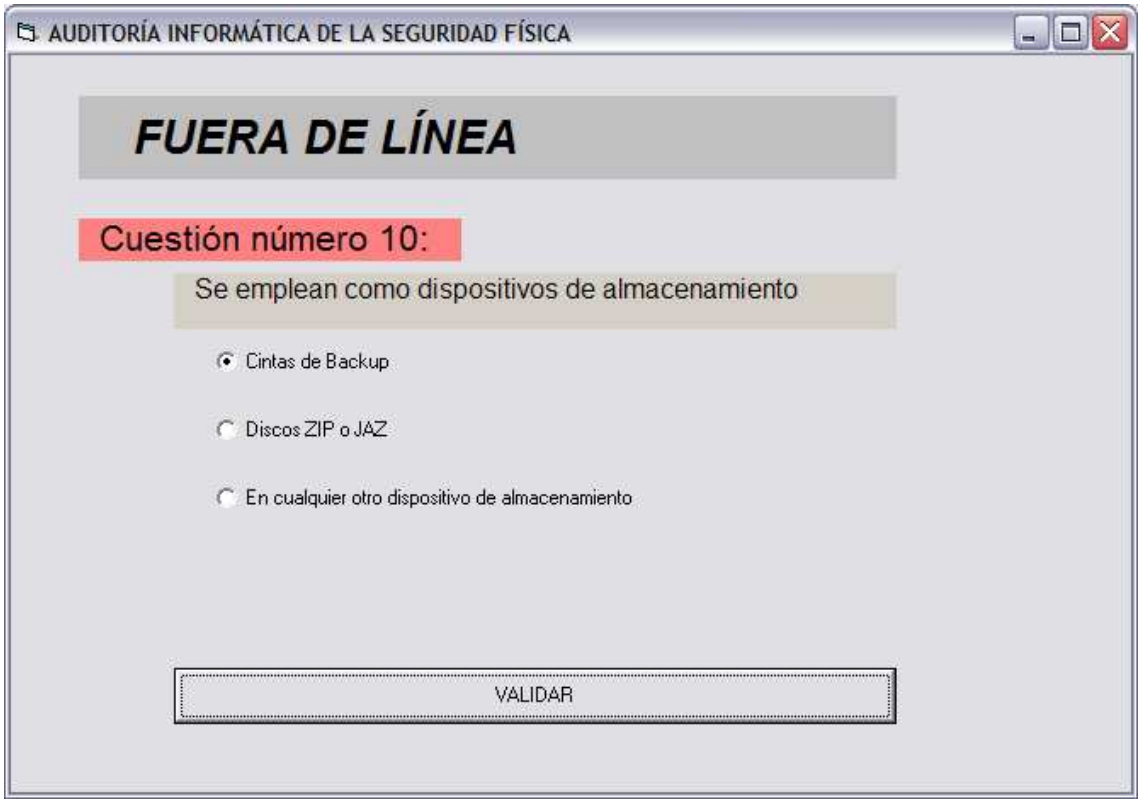

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
FUERA DE LÍNEA
Cuestión número 5:
Existe un sistema de copiado fuera de línea
Sí
No
VALIDAR

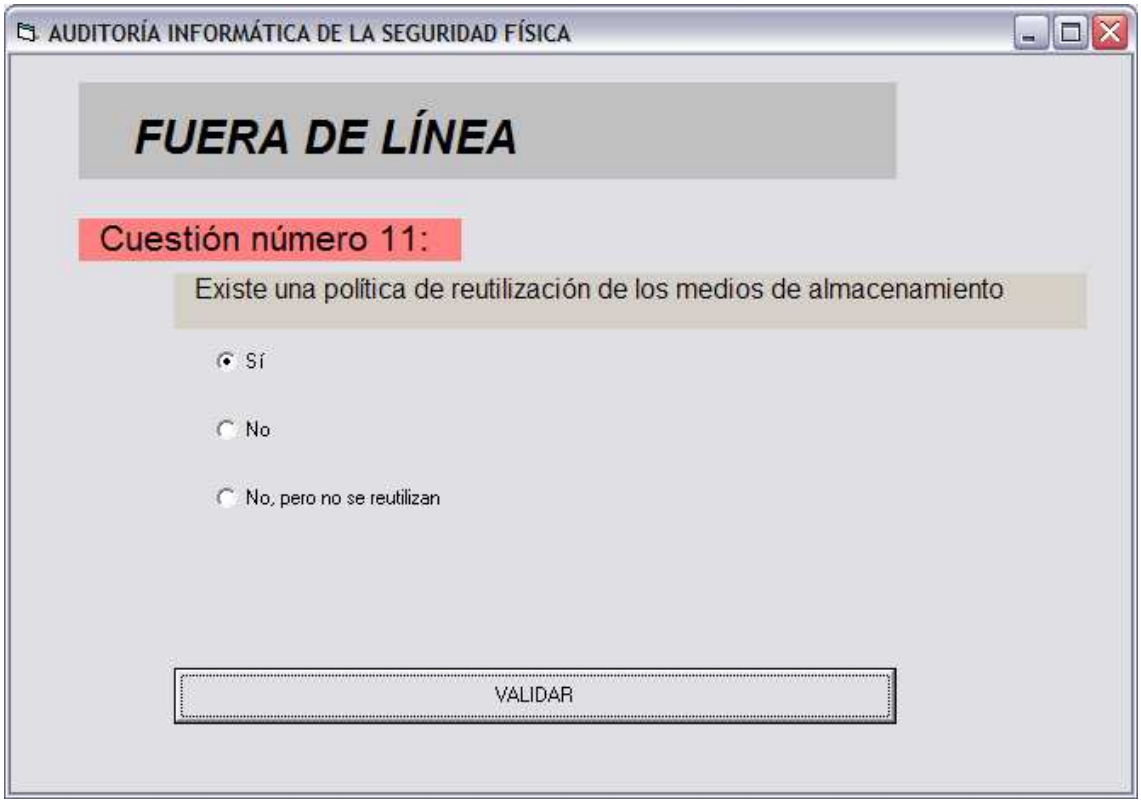

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
FUERA DE LÍNEA
Cuestión número 6:
Los sistemas de lectura-escritura están considerados como críticos
Sí
No
VALIDAR

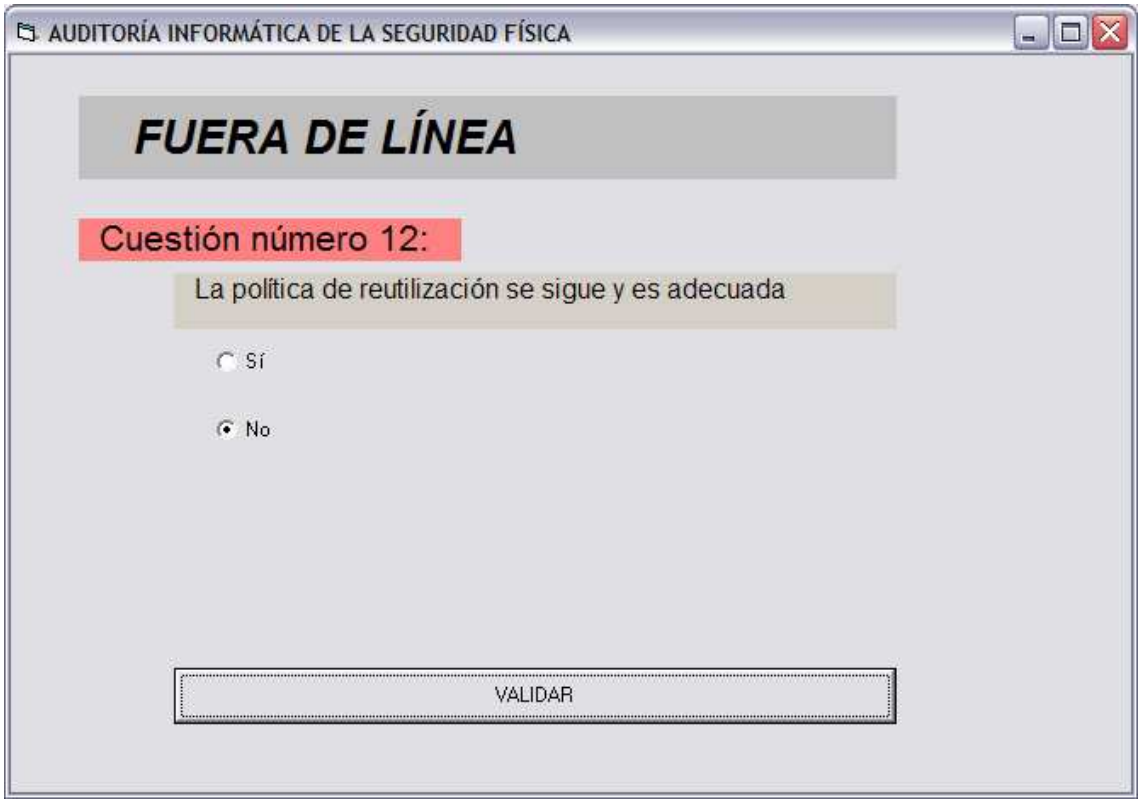

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
FUERA DE LÍNEA
Cuestión número 7:
Se han estudiado las diferentes técnicas para reducir el tiempo de copiado
Sí y se aplican con éxito
Sí, pero no se aplican correctamente
No
VALIDAR

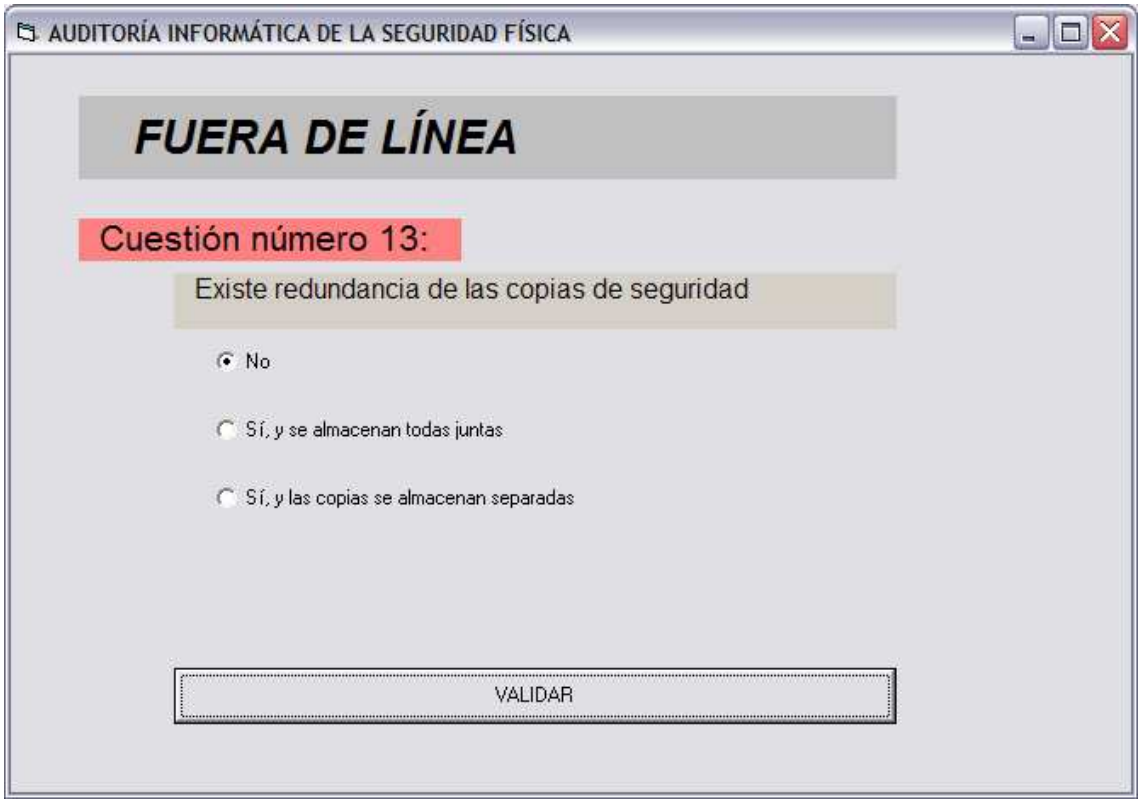

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
FUERA DE LÍNEA
Cuestión número 8:
Se emplea la política de compiado más adecuada (total, incremental, etc.)
Sí
No
No se ha estudiado
VALIDAR

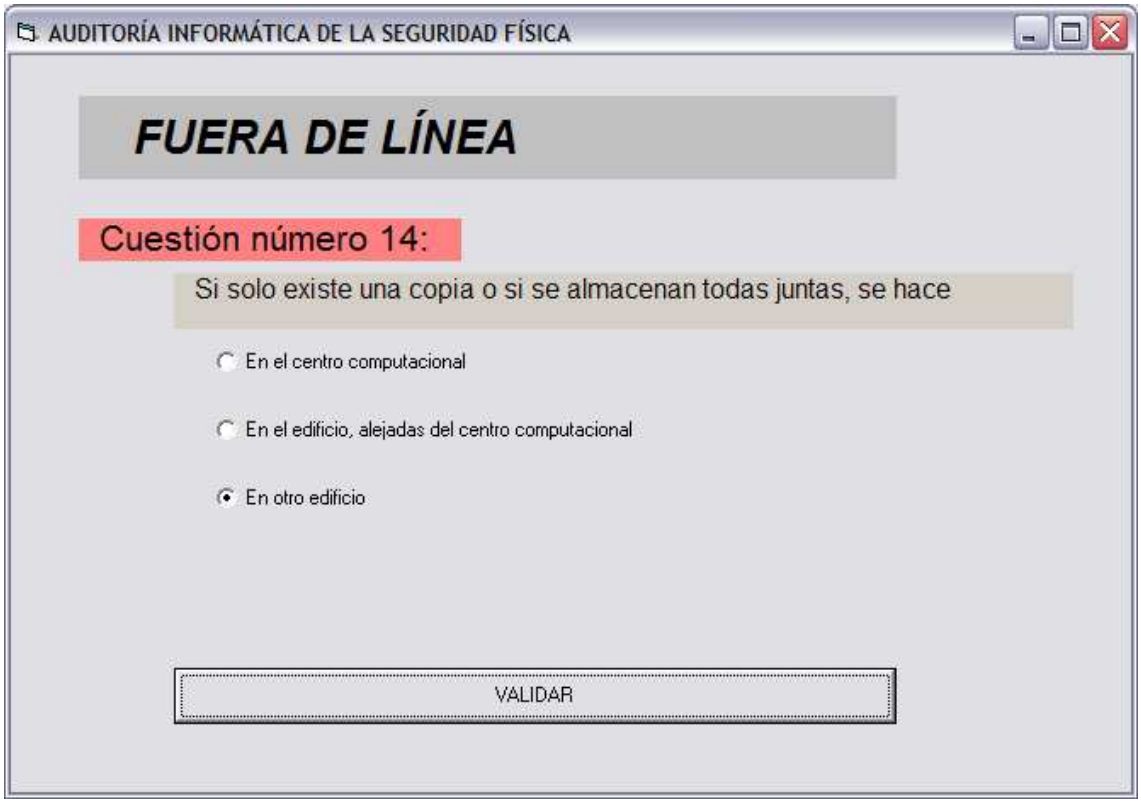

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
FUERA DE LÍNEA
Cuestión número 9:
Se han estudiado las distintas alternativas de medios de almacenamiento
Sí
No
VALIDAR

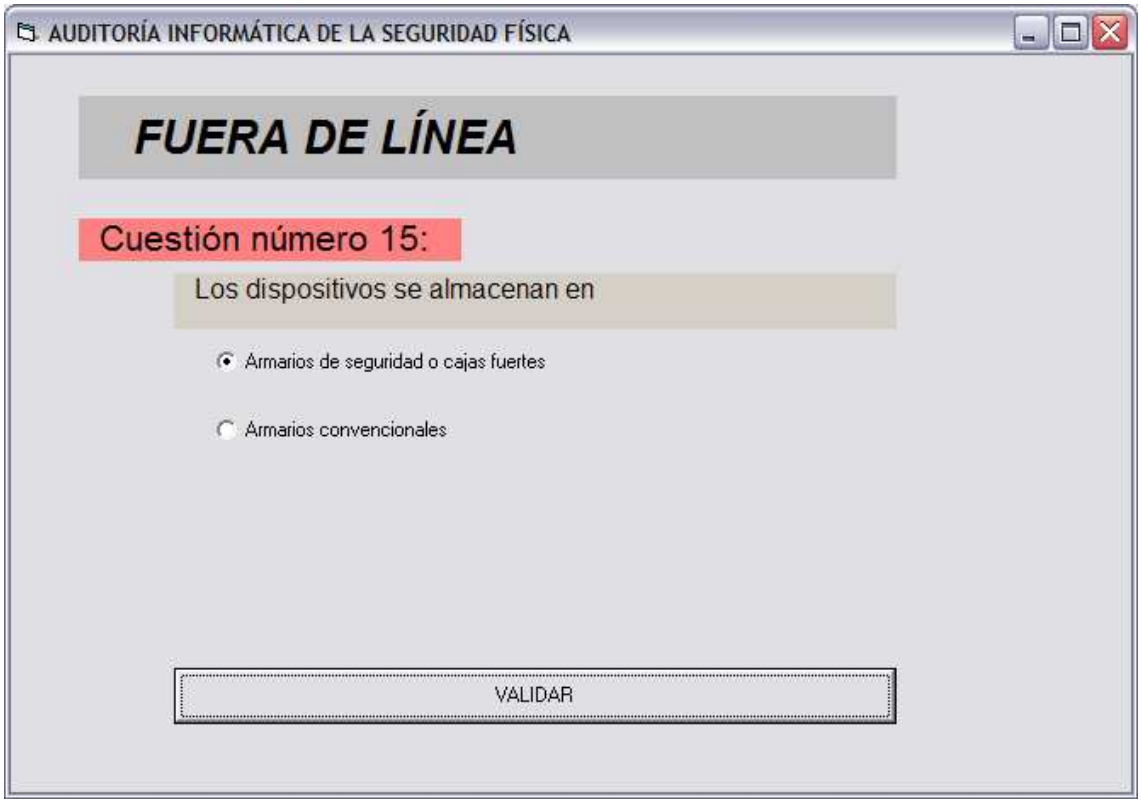

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
FUERA DE LÍNEA
Cuestión número 10:
Se emplean como dispositivos de almacenamiento
Cintas de Backup
Discos ZIP o JAZ
En cualquier otro dispositivo de almacenamiento
VALIDAR

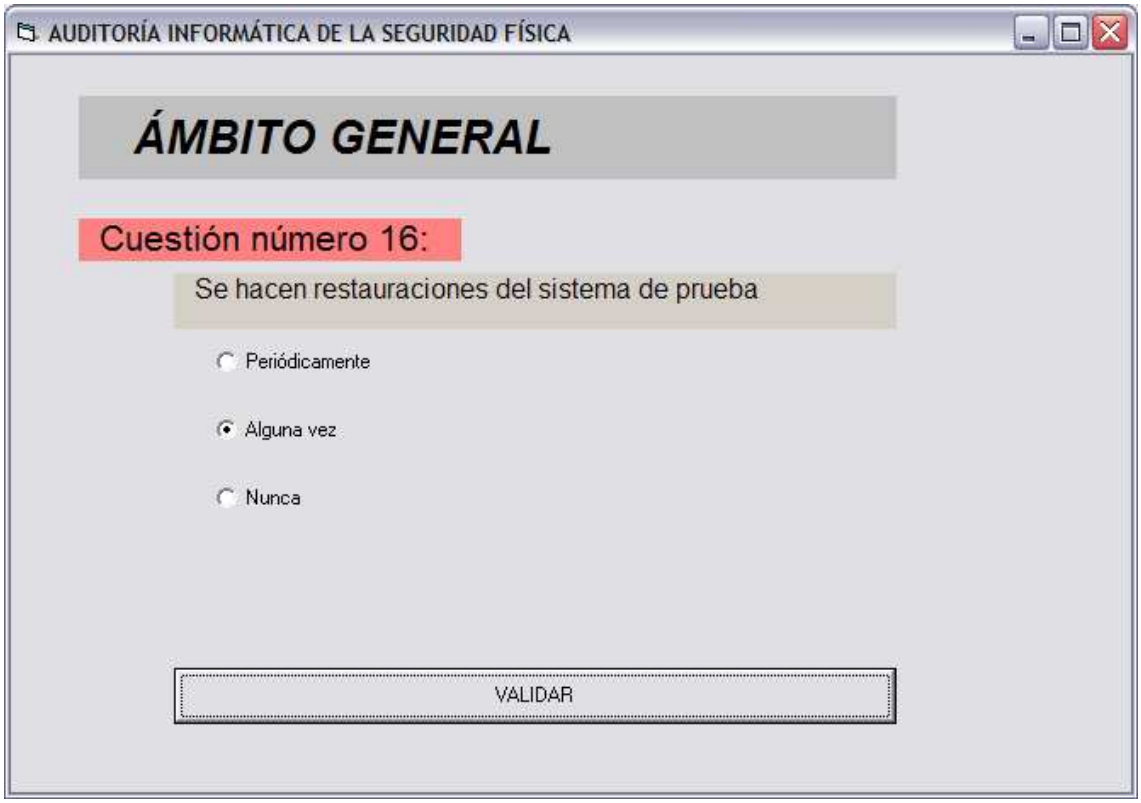

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
FUERA DE LÍNEA
Cuestión número 11:
Existe una política de reutilización de los medios de almacenamiento
Sí
No
No, pero no se reutilizan
VALIDAR

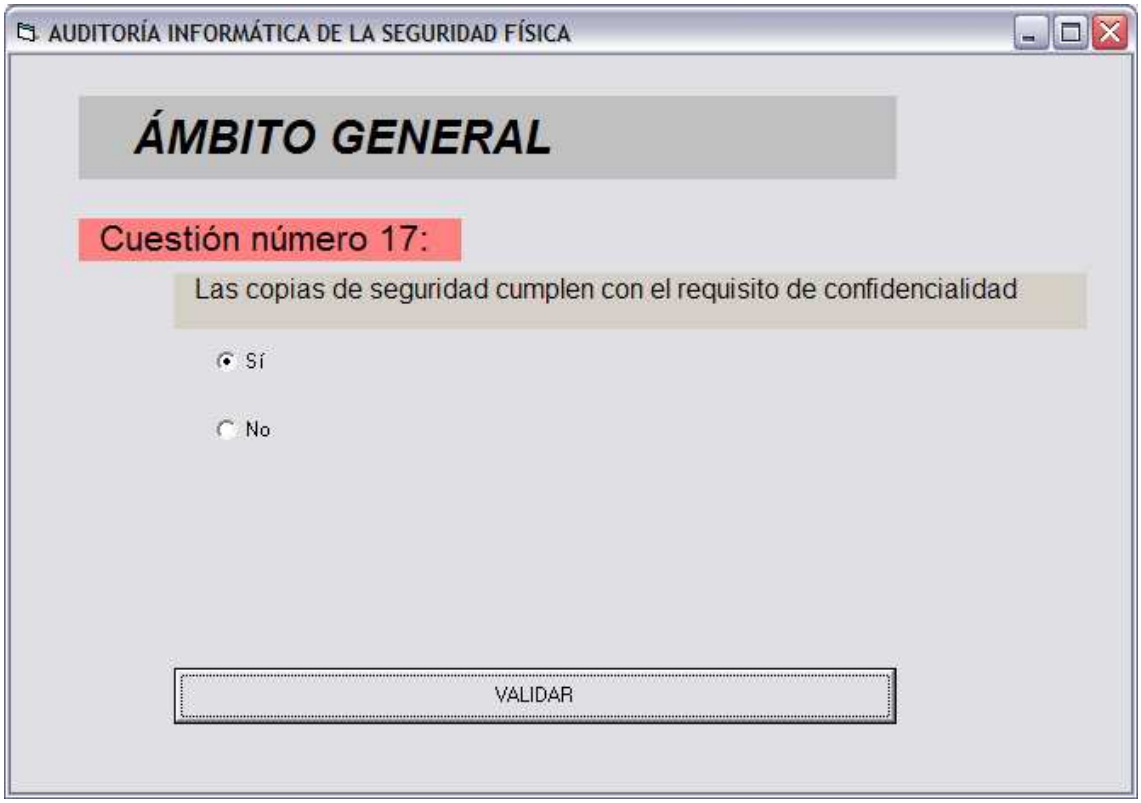

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
FUERA DE LÍNEA
Cuestión número 12:
La política de reutilización se sigue y es adecuada
Sí
No
VALIDAR

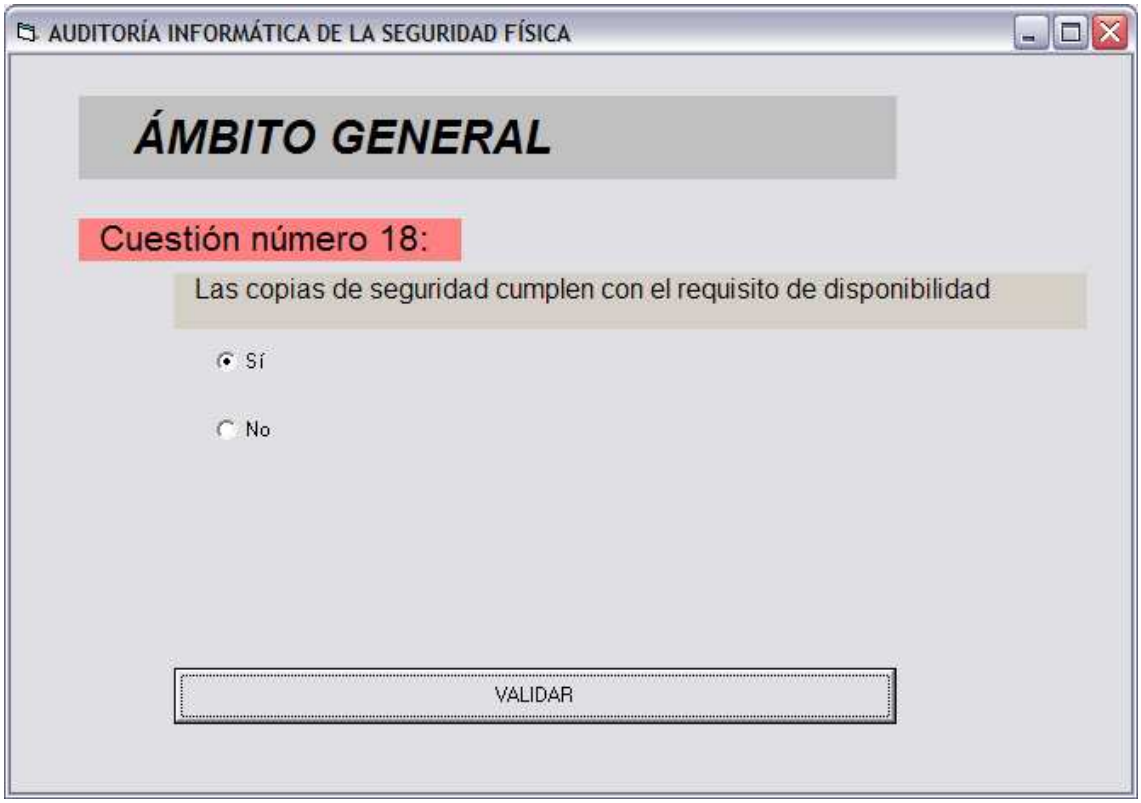

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
FUERA DE LÍNEA
Cuestión número 13:
Existe redundancia de las copias de seguridad
No
Sí, y se almacenan todas juntas
Sí, y las copias se almacenan separadas
VALIDAR

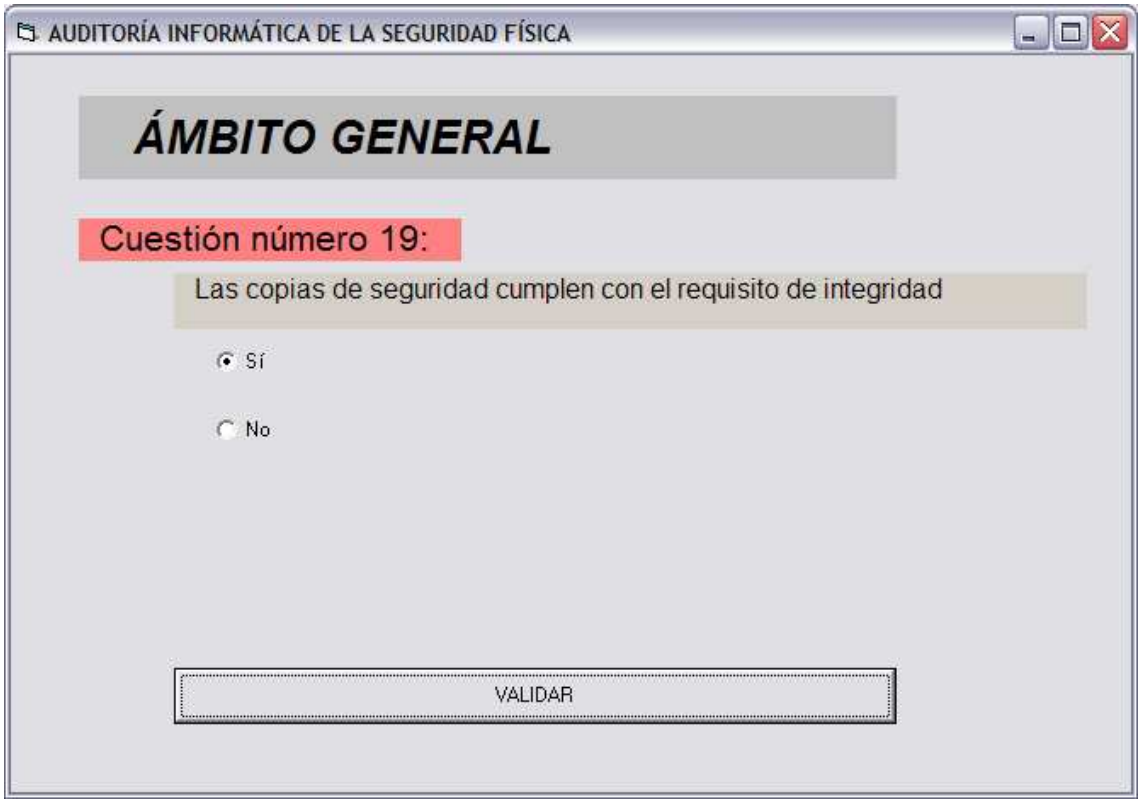

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
FUERA DE LÍNEA
Cuestión número 14:
Si solo existe una copia o si se almacenan todas juntas, se hace
En el centro computacional
En el edificio, alejadas del centro computacional
En otro edificio
VALIDAR

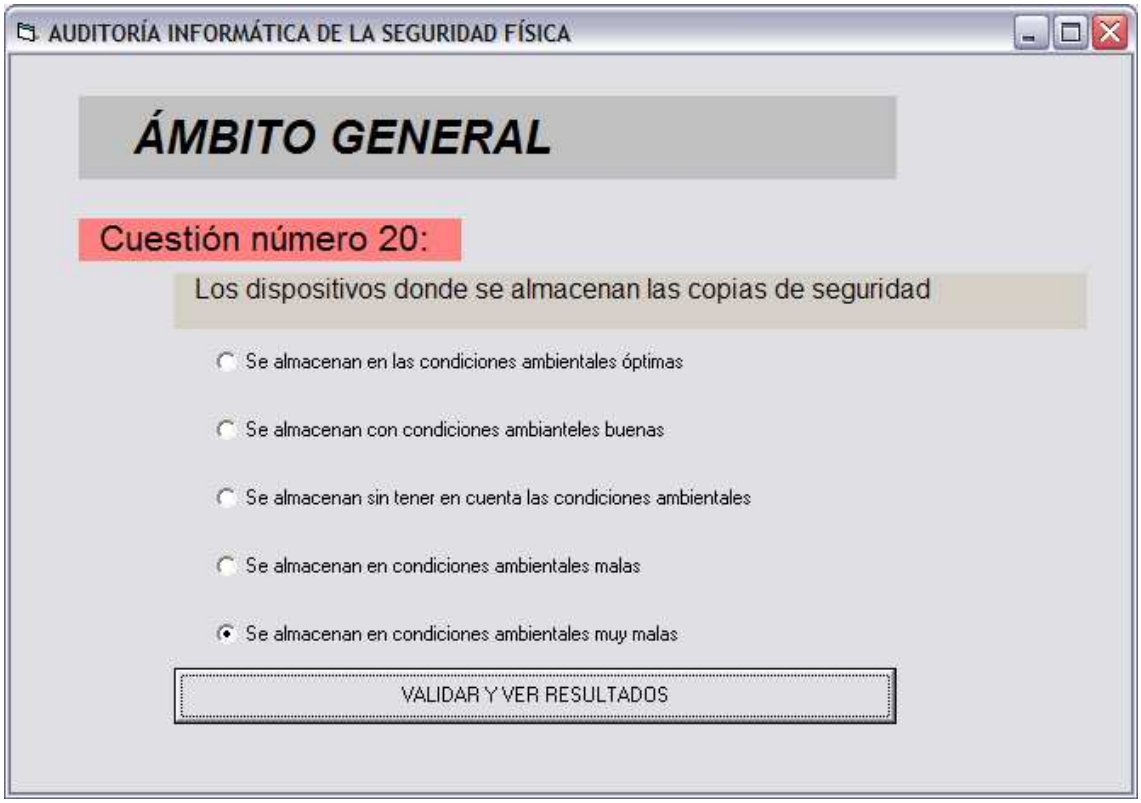

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
FUERA DE LÍNEA
Cuestión número 15:
Los dispositivos se almacenan en
Armarios de seguridad o cajas fuertes
Armarios convencionales
VALIDAR


AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
ÁMBITO GENERAL
Cuestión número 16:
Se hacen restauraciones del sistema de prueba
Periódicamente
Alguna vez
Nunca
VALIDAR


AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
ÁMBITO GENERAL
Cuestión número 17:
Las copias de seguridad cumplen con el requisito de confidencialidad
Sí
No
VALIDAR

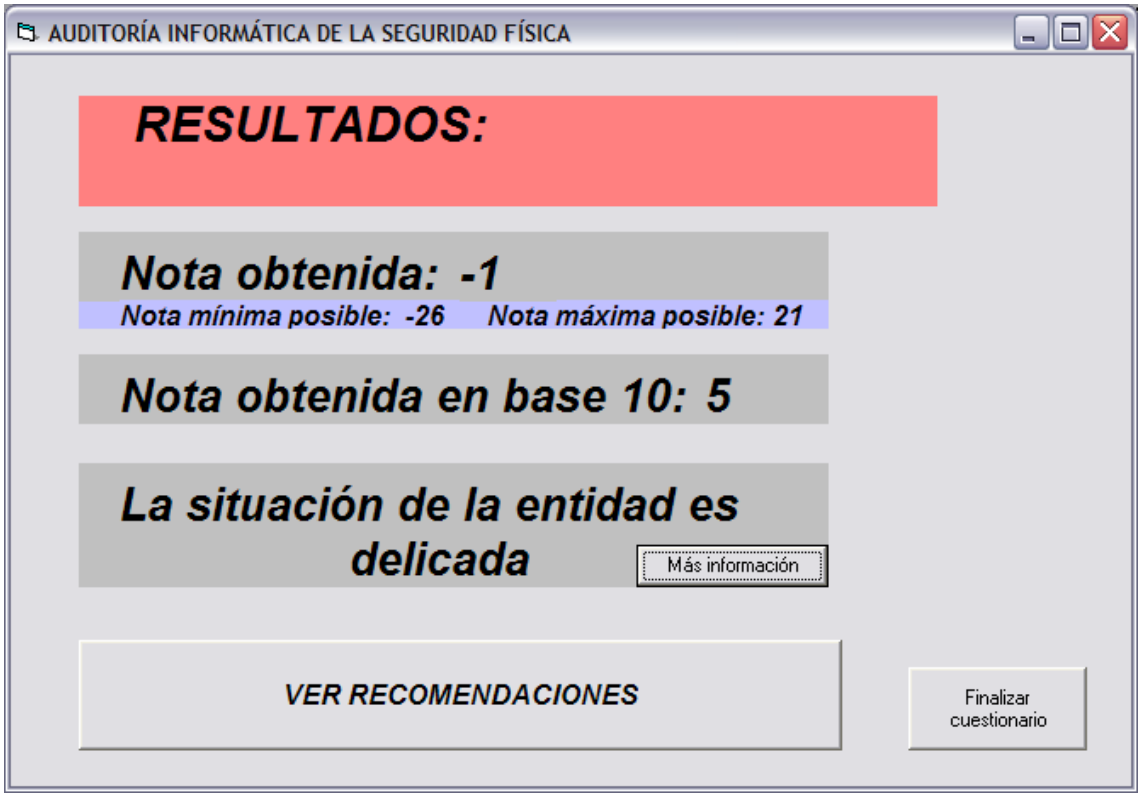

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
ÁMBITO GENERAL
Cuestión número 18:
Las copias de seguridad cumplen con el requisito de disponibilidad
Sí
No
VALIDAR

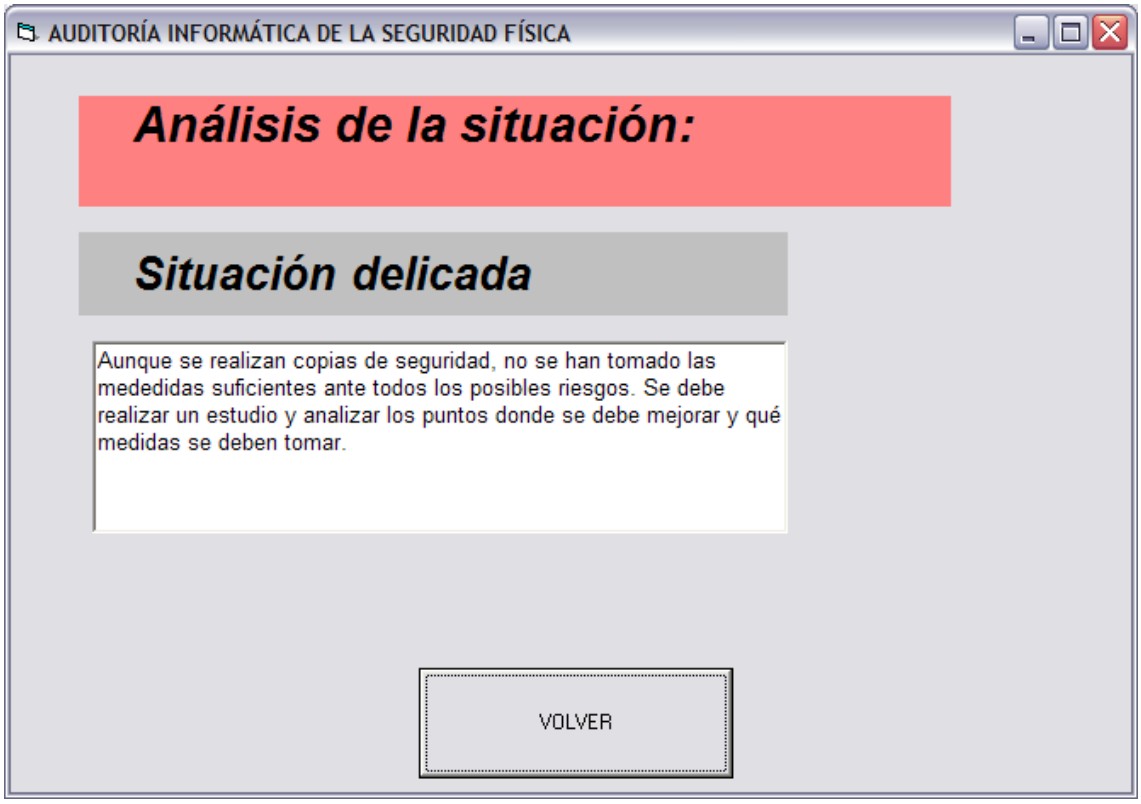

AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
ÁMBITO GENERAL
Cuestión número 19:
Las copias de seguridad cumplen con el requisito de integridad
Sí
No
VALIDAR


AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
ÁMBITO GENERAL
Cuestión número 20:
Los dispositivos donde se almacenan las copias de seguridad
Se almacenan en las condiciones ambientales óptimas
Se almacenan con condiciones ambianteles buenas
Se almacenan sin tener en cuenta las condiciones ambientales
Se almacenan en condiciones ambientales malas
Se almacenan en condiciones ambientales muy malas
VALIDAR Y VER RESULTADOS

c) Resultados

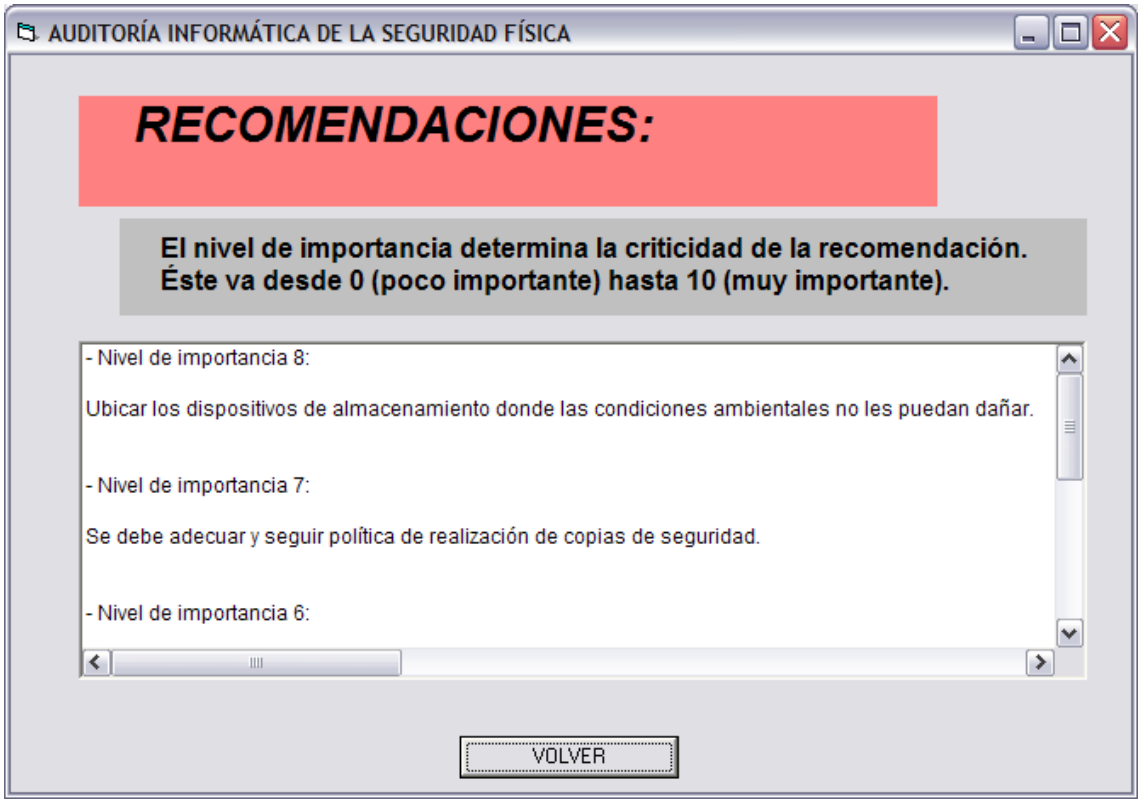
Como se puede apreciar, la nota obtenida en base 10 es un 5, pero el coeficiente de la entidad es negativo, por lo que existen riesgos sin cubrir. Esto es así porque, aunque se realizan copias de seguridad y se ha implantado una política adecuada, ésta no se sigue correctamente y además se han descuidado factores muy importantes, como las condiciones donde se almacenan las cintas de backup.

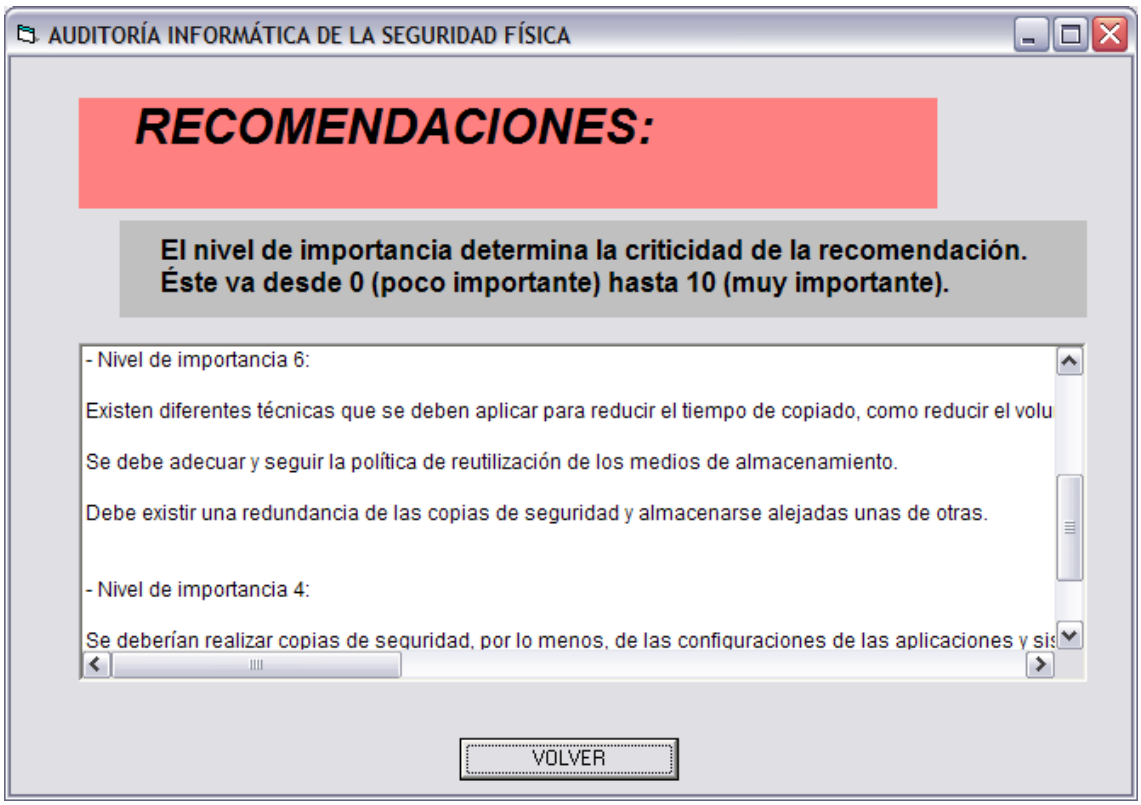


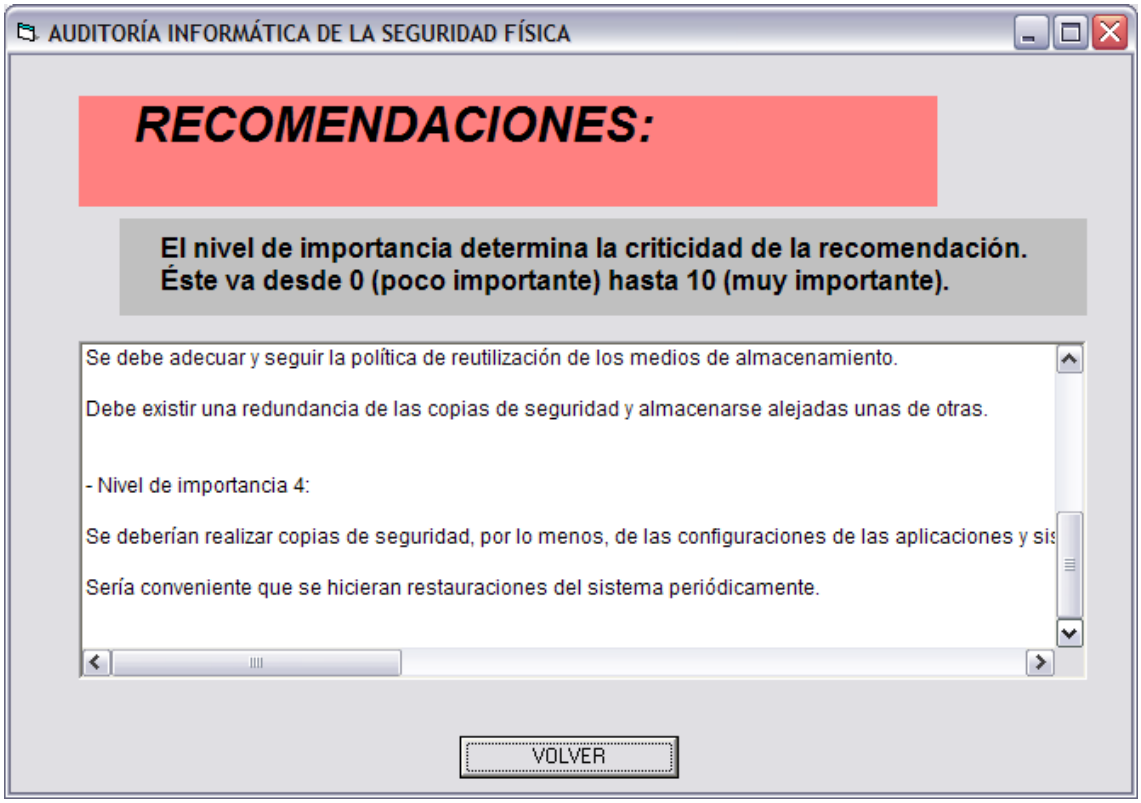


d) Recomendaciones

Como se puede apreciar, y puesto que existen muchos factores que no se han tenido en cuenta o que se realizan de una forma inadecuada, se dan un buen numero de recomendaciones que se deberán seguir para reducir los riesgos.


AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
RECOMENDACIONES:
El nivel de importancia determina la criticidad de la recomendación.
Éste va desde 0 (poco importante) hasta 10 (muy importante).
- Nivel de importancia 8:
Ubicar los dispositivos de almacenamiento donde las condiciones ambientales no les puedan dañar.
- Nivel de importancia 7:
Se debe adecuar y seguir política de realización de copias de seguridad.
- Nivel de importancia 6:
VOLVER


AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
RECOMENDACIONES:
El nivel de importancia determina la criticidad de la recomendación.
Éste va desde 0 (poco importante) hasta 10 (muy importante).
- Nivel de importancia 6:
Existen diferentes técnicas que se deben aplicar para reducir el tiempo de copiado, como reducir el volu
Se debe adecuar y seguir la política de reutilización de los medios de almacenamiento.
Debe existir una redundancia de las copias de seguridad y almacenarse alejadas unas de otras.
- Nivel de importancia 4:
Se deberían realizar copias de seguridad, por lo menos, de las configuraciones de las aplicaciones y sis
VOLVER


AUDITORÍA INFORMÁTICA DE LA SEGURIDAD FÍSICA
RECOMENDACIONES:
El nivel de importancia determina la criticidad de la recomendación.
Éste va desde 0 (poco importante) hasta 10 (muy importante).
Se debe adecuar y seguir la política de reutilización de los medios de almacenamiento.
Debe existir una redundancia de las copias de seguridad y almacenarse alejadas unas de otras.
- Nivel de importancia 4:
Se deberían realizar copias de seguridad, por lo menos, de las configuraciones de las aplicaciones y sis
Sería conveniente que se hicieran restauraciones del sistema periódicamente.
VOLVER

8 - CONCLUSIONES

Para concluir este trabajo, se deben comentar ciertos aspectos valorativos. Empezaremos por hablar de lo que me ha aportado a mí el realizar el trabajo, y qué aporto yo con el mismo. Comentaremos el tiempo que he dedicado en realizarlo y las posibles líneas de investigación que dejo abiertas.

a) Qué me ha aportado

De lo primero que tengo que hablar a la hora de analizar lo que me ha aportado el realizar este trabajo es de la capacidad para plantearme el cómo realizar un proyecto de esta magnitud, cómo estructurarlo y qué debía incluir en el mismo y qué no. He tenido que realizar un análisis global para, partiendo de cero, conseguir un trabajo con una estructura sólida y unas partes bien definidas.

También, y debido a la alta carga documental del trabajo, he realizado una gran búsqueda de información, tanto en la Red como en la biblioteca, lo que me ha permitido adquirir cierta destreza. Una vez recopilada la información, comenzaba el proceso de selección e integración, donde era necesaria una gran capacidad de esquematización y abstracción.

He adquirido conocimientos sobre como se elaboran y estructuran las normas y procedimientos, así como el contenido de algunas en concreto, ya que durante el desarrollo de este trabajo he manejado ciertas leyes, normas UNE y estándares ISO.

Para el desarrollo del trabajo se ha empleado el procesador de texto ***Microsoft Word XP***, del que sólo conocía las funciones básicas. Al haber finalizado el trabajo he aprendido a manejarlo de una manera mucho más significativa.

Para el desarrollo de la aplicación se ha empleado ***Microsoft Visual Basic 6.0***, lenguaje que no había manejado nunca. Esto me ha permitido adquirir conocimientos nuevos sobre este lenguaje, así como refrescar los ya adquiridos en la carrera sobre programación, ya que hacía bastante tiempo que no los ponía en práctica.

Para finalizar debo recalcar, que al margen de los conocimientos puntuales que haya podido adquirir, lo más importante para mí ha sido el planificar, estructurar y llevar a cabo un trabajo como éste partiendo desde cero, por supuesto, con la ayuda de mi tutor, Miguel Ángel Ramos.

b) Qué he aportado

Como mentaba en la introducción, en este trabajo se ha intentado hacer notar la gran importancia que ha adquirido la información en la sociedad actual, y consecuentemente los sistemas que se emplean para almacenarla y tratarla. Puesto que en muchas ocasiones estos sistemas forman parte de las llamadas *nuevas tecnologías*, es frecuente el desconocimiento, por parte de los usuarios, de las necesidades de seguridad de estos sistemas, así como de las consecuencias que puede tener para la entidad su pérdida o deterioro.

Por ello se ha realizado una recopilación de los elementos que se deben asegurar, las posibles amenazas que existen y los sistemas disponibles para minimizar los riesgos. Esta recopilación parte de un nivel muy básico, por lo que puede ser fácilmente entendida por cualquier persona.

Especialmente se ha profundizado en la seguridad física y todos sus aspectos relacionados con los sistemas de información, analizando los dispositivos más vulnerables y críticos, las amenazas más comunes, los factores que pueden hacer que aumente el nivel de riesgo y los sistemas, procedimientos y dispositivos más comunes que podemos aplicar para reducir al máximo la probabilidad de que las amenazas se conviertan en daños o pérdidas.

Además se ha realizado un pequeño análisis de qué es y cómo funciona una auditoría informática, concepto que mucha gente, aún hoy en día, desconoce. He analizado y puesto de manifiesto, además, las peculiaridades de la auditoría informática de la seguridad física.

Para la elaboración de la auditoría informática sobre la seguridad física, se ha realizado un cuestionario. Como ya se ha comentado, éste se puede emplear en distintas fases del proceso de auditoría, contando, además, con unos pesos o coeficientes que se podrán modificar y adecuar para distintas auditorías.

Este cuestionario ha sido, además, la base para el prototipo de aplicación que se ha desarrollado. Esta aplicación se puede emplear en la realización de la auditoría para facilitar el trabajo de los auditores, así como para obtener rápida y automáticamente los resultados sobre la situación de la entidad y las recomendaciones que se deben dar.

Por tanto, para finalizar debería decir que lo que principalmente he aportado es poner de manifiesto la importancia de la información y las principales medidas, a nivel de seguridad física, que se deben adoptar, así como aclarar y explicar conceptos básicos relacionados, muchos de ellos aún desconocidos por mucha gente.

c) Tiempo dedicado

Para poder analizar el tiempo que he dedicado a la realización del proyecto debo diferenciar tres grandes fases de trabajo:

En la primera fase busqué un tema apropiado para realizar sobre el que realizar el proyecto. Una vez que lo obtuve analicé que es lo que debía abarcar que no, como estructurarlo, etc. Durante el transcurso de esta fase los momentos de trabajo eran puntuales y dispersos en el tiempo, por lo que estimo una duración total de 20 horas.

La segunda fase se extendió mucho en el tiempo. A lo largo de ésta, y mientras empezaba a documentarme y recopilar información, concreté aún más que debía hacer y cómo hacerlo. El trabajo no era diario pero iban aumentando las horas de trabajo, por lo que estimo una duración de unas 60 horas.

La tercera y última fase ha sido la más extensa, tanto en el tiempo como en horas de trabajo. Ya tenía clara la estructura del proyecto, como hacerlo y qué debía abarcar, así como cierta soltura a la hora de recabar, analizar e integrar la información. Esta fase ha durado unos 4 meses, realizando un trabajo diario de unas 4 horas de media, por tanto estimo unas 400 horas.

Resumiendo, una aproximación de las horas de trabajo dedicadas al proyecto sería 480 horas.

d) Líneas abiertas a investigación

Una vez que he acabado el trabajo, puedo decir que quedan abiertas algunas líneas para futuras investigaciones.

La primera que debo comentar es la de actualización del trabajo. Parece obvio que en poco tiempo los sistemas y dispositivos de los que se habla en este trabajo quedarán desfasados, ya que debido a la alta demanda, la tecnología informática y de seguridad avanza a pasos agigantados.

Otra posible línea de investigación sería la de realizar un trabajo similar pero enfocado a la seguridad lógica.

También se podría profundizar en cualquiera de los puntos tratados en este trabajo, como las copias de seguridad, los incendios, la energía eléctrica, etc., ya que como he comentado anteriormente, todos los aspectos se tratan de una manera general.

Lógicamente, es posible que haya pasado sistemas, dispositivos o factores por alto, por lo que otra línea que queda abierta es la de añadir o modificar posibles errores u omisiones que haya podido realizar.

La aplicación informática que he desarrollado es sólo un prototipo, por lo que he implementado solamente la parte de las copias de seguridad, por lo que una línea que queda abierta es la de implementar el resto de apartados.

Como ya he comentado, la aplicación que he desarrollado es sólo un prototipo, por lo que otra línea de investigación que queda abierta sería la de añadir nuevas funcionalidades a la aplicación, como poder cambiar los pesos de las preguntas, mostrar menús de ayuda en pantalla, almacenar los resultados en una base de datos, etc.

9 - BIBLIOGRAFÍA

AENOR. *Recopilación de Normas AENOR contra incendios. Tomos 1, 2 y 3*. Madrid: AENOR, 1998.

AENOR. *Sistemas de gestión de la calidad*. ISO 9001-2000. Madrid: AENOR, 2000.

ARGÜELLO, Felipe. *Dispositivos de Alarma de Incendio*. España: 1999

DAVIS, Harold. *Microsoft Visual Basic 6*. Madrid: Anaya Multimedia, 1999. ISBN 84-415-0818-6.

ESPAÑA. MINISTERIO DE ADMINISTRACIONES PÚBLICAS. *Magerit versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid: Ministerio de Administraciones Públicas, 2005.

Information System Audit and Control Foundation. *COBIT, Objetivos de Control para la Información y Tecnologías Afines.* USA: Information System Audit and Control Foundation, 1998. ISBN 0-9629440-4-1

ISO. *Information technology - Code of practice for information security management*. ISO-IEC 17799-2000. Switzerland: ISO, 2005.

LÓPEZ, José María. *Seguridad Física COMO*. USA: bgSEC, 2002.

RAMOS GONZÁLEZ, Miguel Ángel. *Auditoría Informática*. Madrid: Universidad Carlos III de Madrid, 2003.

Seguridad y protección de la información. Madrid, Universidad Carlos III de Madrid, 2001.

Servicio Provincial de Incendios de la Diputación de Albacete (S.E.P.E.I.). *Manual S.E.P.E.I de bomberos*. Albacete: Ardit.net, 2003.

VILLALÓN HUERTA, Antonio. *Seguridad en UNIX y Redes, Versión 2.1*. España: 2002.

Páginas Web consultadas:

Agencia Española de Protección de Datos
http://www.agpd.es

Asociación Deportivo Cultural Bomberos de Navarra.
http://www.bomberosdenavarra.com

Belt Iberica S.A. Sistemas de seguridad global.
http://www.belt.es

Buscador Google.
http://www.google.es

Enciclopedia Wikipedia.
http://www.wikipedia.org

Generadores eléctricos BRAVO S.L.
http://www.gebravo.com

Kompusur S.A. Sistemas de alarma.
http://x-28.com

L.P.G. Técnicas en extinción de incendios S.A.
http://www.lpg.es

Ministerio de Trabajo y Asuntos Sociales. Notas técnicas de prevención de incendios.
http://www.mtas.es/insht/ntp/Incendios.htm

Monografías.com.
http://www.monogrfias.com

New SAI S.L. Sistemas de alimentación ininterrumpida.
http://www.newsai.es

Real Academia Española.
http://www.rae.es

Real Casa de la Moneda. Fábrica Nacional de Moneda y Timbre.
http://www.fnmt.es/es/html/ho-ho.asp

Red IRIS. Plan nacional de I+D.
http://www.rediris.es

Riesgos y seguridad en los sistemas de información. Auditoría informática.
http://ciberconta.unizar.es/LECCION/SEGURO/inicio.html

S.I. Alerta. S.L. Sistemas de alarma.
http://www.seguralerta.com

Secretaría del Consejo Superior de Administración Electrónica.
http://www.csi.map.es

Security Management Online. Physical Security.
http://www.securitymanagement.com/Physical_security.html

Skylink Seguridad. Sistemas de seguridad.
http://www.skylinkseguridad.com

Solocursos.net. Guía online de cursos.
http://www.solocursos.net